4ipnet®
for your IP network

User's Manual

WHG303 V1.00

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission of 4IPNET, INC.

Disclaimer

4IPNET, INC. does not assume any liability arising out the application or use of any products, or software described herein. Neither does it convey any license under its parent rights not the parent rights of others. 4IPNET further reserves the right to make changes in any products described herein without notice. The publication is subject to change without notice.

Trademarks

4IPNET (4ipnet) is a registered trademark of 4IPNET, INC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

© 2008 4IPNET, INC.

Table of Contents

1. Before You Start **1**
1.1 Preface 1
1.2 Document Conventions 1
2. System Overview **2**
2.1 Introduction of 4ipnet WHG303 2
2.2 System Concept 2
2.3 Hardware Specification 3
3. Installation **4**
3.1 Hardware Installation 4
3.1.1 System Requirements 4
3.1.2 Package Contents 4
3.1.3 Panel Function Descriptions 5
3.1.4 Installation Steps 6
3.2 Software Configuration 7
3.3.1 Instruction of Web Management Interface 7
3.3.2 Setup Wizard 13
3.3.3 User Login Portal Page 16
4. Web Interface Configuration **17**
4.1 System Configuration 19
4.1.1 General 20
4.1.2 WAN1 Configuration 23
4.1.3 WAN2 Configuration 25
4.1.4 WAN Traffic Settings 27
4.1.5 LAN Port Mapping 29
4.1.6 Service Zones 33
4.2 User Authentication 39
4.2.1 Authentication Configuration 40
4.2.2 Black List Configuration 70
4.2.3 Group Configuration 71
4.2.4 Policy Configuration 75
4.2.5 Additional Configuration 84
4.3 AP Management 87
4.3.1 AP List 88
4.3.2 AP Discovery 94
4.3.3 Adding 97
4.3.4 Template Settings 98

© 2008 4IPNET, INC.

4.3.5 Firmware Upload 99
4.3.6 AP Upgrade 100
4.3.7 WDS Management 101
4.4 Network Configuration 102
4.4.1 Network Address Translation 103
4.4.2 Privilege List 106
4.4.3 Monitor IP List 108
4.4.4 Walled Garden List 109
4.4.5 Walled Garden Ad List 110
4.4.6 Proxy Server Properties 111
4.4.7 Dynamic DNS 112
4.4.8 Client Mobility 113
4.4.9 VPN Configuration 114
4.5 Utilities 116
4.5.1 Change Password 117
4.5.2 Backup/Restore Settings 121
4.5.3 Firmware Upgrade 122
4.5.4 Restart 123
4.5.5 Network Utilities 124
4.6 Status 125
4.6.1 System Status 126
4.6.2 Interface Status 128
4.6.3 Routing Table 130
4.6.4 Online Users List 132
4.6.5 Users Logs 133
4.6.6 E-mail & SYSLOG 136
4.7 Help 138
Appendix A. Accepting Payment via Authorize.Net 139
Appendix B. Accepting Payment via PayPal 149
Appendix C. Accepting Payment via SecurePay 159
Appendix D. Service Zone Deployment Example 170
Appendix E. Proxy Setting 183
Appendix F. Session Limit and Session Log 188
Appendix G. Network Configuration on PC & User Login 190
Appendix H. Console Interface 206
Appendix I. Local VPN 209
Appendix J. Customizable Pages 217
Appendix K. RADIUS Accounting 221

© 2008 4IPNET, INC.

1. Before You Start

1.1 Preface

This manual is for hotspot owners or network administrators to set up a network environment using the 4ipnet WHG303 system. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

1.2 Document Conventions

	Represents essential steps, actions, or messages that should not be ignored.
Note:	Contains related information that corresponds to a topic.
	Indicates that clicking this button will return to the homepage of this section.
	Indicates that clicking this button will apply all of your settings.
	Indicates that clicking this button will clear what you have set before these settings are applied.

© 2008 4IPNET, INC.

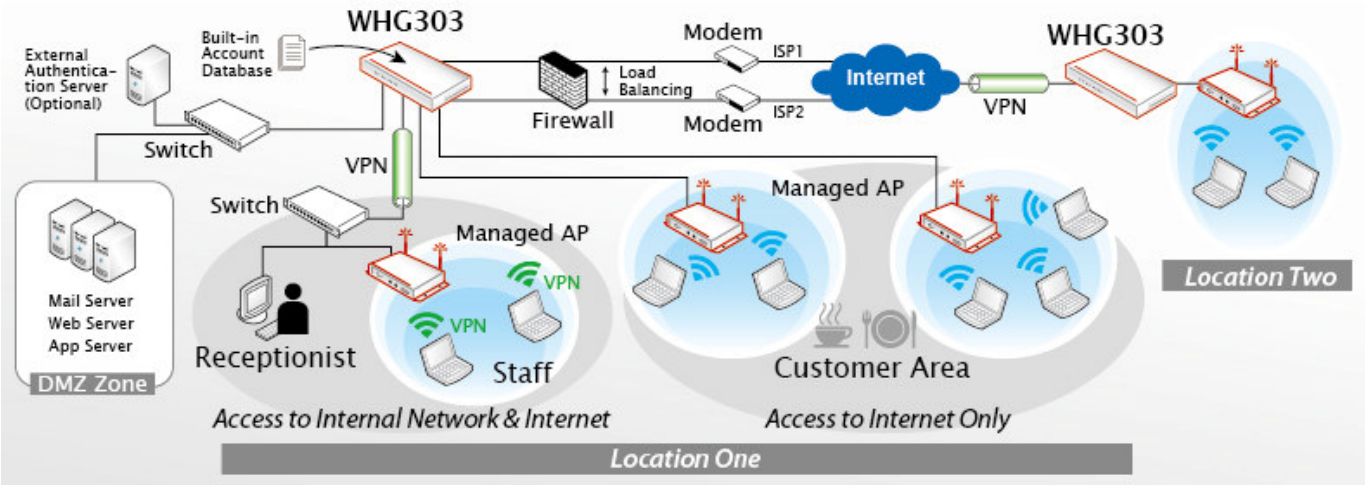
2. System Overview

2.1 Introduction of 4ipnet WHG303

4ipnet WHG303 Secure WLAN Controller is an ideal solution for small to medium hotspot deployments, such as in hotels, hospitals, convention centers, libraries, airport terminals, and MDUs/MTUs. The WHG303 integrates "secure access control", "visitor account provisioning", "flexible accounting and billing", and "high-speed secure wireless connection" into one box to fulfill the needs demanded by a public wireless network. It also provides advanced functions suitable for larger networks to accommodate more users with multiple APs to cover a wider service area.

2.2 System Concept

4ipnet WHG303 is capable of managing user authentication, authorization and accounting. The user account information is stored in the local database or a specified external database server. Featured with user authentication and integrated with external payment gateway, WHG303 allows users to easily pay the fee and enjoy the Internet service using credit cards through **Authorize.net**, **PayPal** or **SecurePay**. With centralized AP management feature, the administrator does not need to worry about how to manage multiple wireless access point devices. Furthermore, WHG303 introduces the concept of Service Zones - multiple virtual networks, each with its own definable access control profiles. This is very useful for hotspot owners seeking to provide different customers or staff with different levels of network services. The following diagram is an example of WHG303 set to manage the Internet and network access services at a hotspot venue.



【*Example: Managed network deployment*】

© 2008 4IPNET, INC.

2.3 Hardware Specification

General

- Form Factor: 19" 1U Rack Mount
- Dimensions (W x D x H): 16.9" x 6.1" x 1.7" (430 mm x 155 mm x 43 mm)
- Weight: 3.3lbs (1.5 kg)
- Operating Temperature: 0 ~ 40 ℃
- Storage Temperature: -20 ~ 65 ℃
- Power: 100~240 VAC, 50/60 Hz
- CE, FCC
- RoHS compliant

Connectors and Display

- WAN Ports: 2 x 10/100BASE-TX RJ-45
- LAN Ports: 4 x 10/100BASE-TX RJ-45
- Console Port: 1 x RS-232 DB9
- LED Indicators: 1 x Power, 1 x Status, 2 x WAN, 4 x LAN

© 2008 4IPNET, INC.

3. Installation

3.1 Hardware Installation

3.1.1 System Requirements

- Standard 10/100BaseT including network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.1.2 Package Contents

The standard package of 4ipnet WHG303 includes:

- 4ipnet WHG303 x 1
- Quick Installation Guide (QIG) x 1
- CD-ROM (with User's Manual and QIG) x 1
- Power Cord x 1
- Power Adaptor (12DC, 2A) x 1
- Cross-over Ethernet RJ-45 Cable x 1
- RS-232 DB9 Console Cable x 1

It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

© 2008 4IPNET, INC.

3.1.3 Panel Function Descriptions

Front Panel

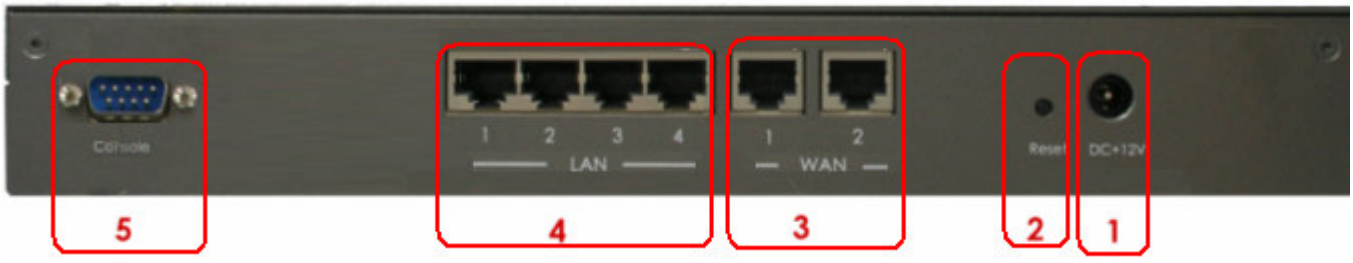
① **Power：** ON indicates the power on, and OFF indicates the power off.

② **Status：** Power and Status both ON indicate system ready, OFF indicates BIOS running, and BLINKING indicates OS running.

③ **WAN：** ON indicates connection, OFF indicates no connection, and BLINKING indicates data transmitting.

④ **LAN：** ON indicates connection, OFF indicates no connection, and BLINKING indicates data transmitting.

Rear Panel



① **DC+12V：** Attach the power adaptor here.

② **Reset：**

Press and hold the Reset button for about 5 seconds and the LED status indicator on the front panel will start to blink before restarting the system.

Press and hold the Reset button for more than 10 seconds and the LED status indicator on the front panel will start to speed up blinking before resetting the system to default configuration.

③ **WAN：**

For connecting to external networks which are not managed by WHG303 via ADSL or Cable Modem, or connecting to a certain LAN of an organization via Switch or Hub.

④ **LAN：**

For connecting to the networks managed by WHG303, such as client networking devices.

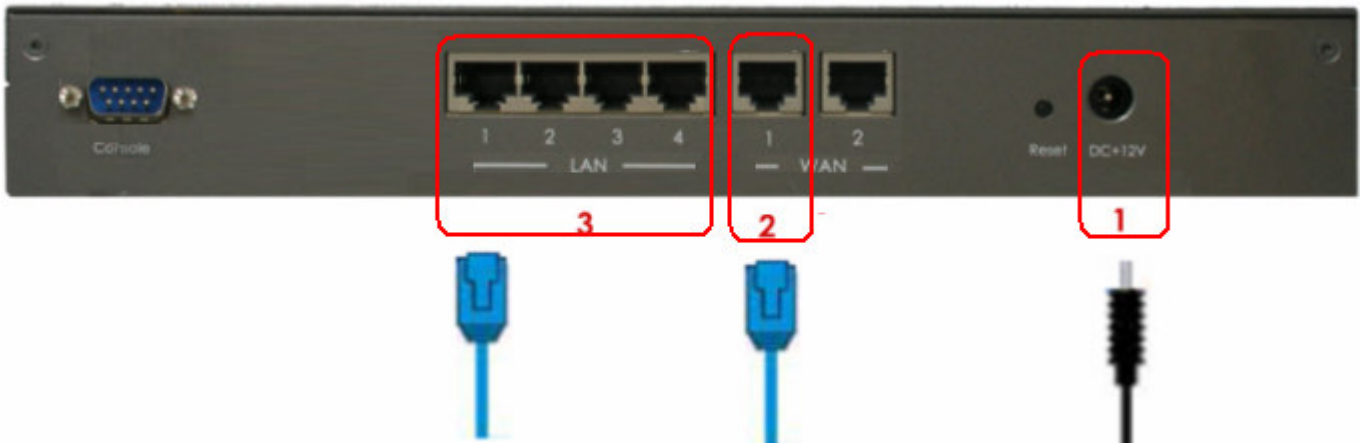
WHG303 supports Service Zone function including Port-Based mode and Tag-Based mode. Under Tag-Based mode, service zones are distinguished by VLAN tagging instead of physical LAN ports, and vise versa. By default, the system is in Port-Based mode and all LAN ports are set to the default service zone.

⑤ **Console：** For displaying text data on an extended monitor via a RS-232 DB9 cable.

© 2008 4IPNET, INC.

3.1.4 Installation Steps

Please follow the steps below to install 4ipnet WHG303:



1. Connect the **Power adapter** to the power socket on the rear panel. The Power LED on the front panel should be ON to indicate a proper connection.

> *Using a non-certified power adapter may damage this system.*

2. Connect an **Ethernet cable** to WAN1 Port on the rear panel. Per your needs, connect the other end of the cable to a networking device such as ADSL modem, cable modem, switch or hub. The WAN1 LED indicator should be ON to indicate a proper connection.

3. Connect an **Ethernet cable** to any LAN Port on the rear panel. Connect the other end of the cable to a PC for configuring the WHG303 system. The LED indicator should be ON to indicate a proper connection.

© 2008 4IPNET, INC.

3.2 Software Configuration

3.3.1 Instruction of Web Management Interface

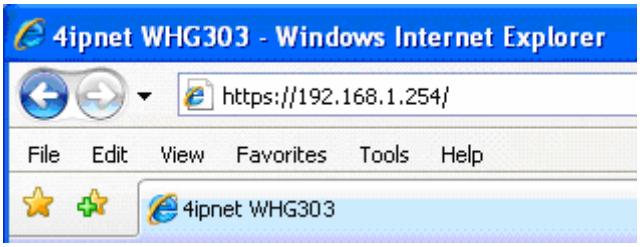
4ipnet WHG303 supports web-based configuration. Upon the completion of hardware installation, WHG303 can be configured through a PC by using its web browser with JavaScript enabled such as Internet Explorer version 6.0.

Step 1:

Set DHCP in TCP/IP of the administrator PC to get an IP address dynamically. Connect the PC to any LAN Port of WHG303. An IP address will be assigned to the PC automatically via the WHG303 built-in DHCP server.

Step 2:

Launch a web browser to access the web management interface of WHG303 by entering **"https://192.168.1.254"** (**"https"** is used for a secured connection) or **"http://192.168.1.254"** in the address field.



Step 3:

The following Administrator Login Page will then appear. Enter **"admin"** (the default value) in the *Username* and *Password* fields, and then click ***Login*** to log in.

Note: If you are unable to get to the login screen, please check the IP address used. The IP address should be in the same subnet of the default gateway. For using static IP in TCP/IP setting, set a static IP address such as 192.168.1.x for your network interface, and then open a new browser again.

© 2008 4IPNET, INC.

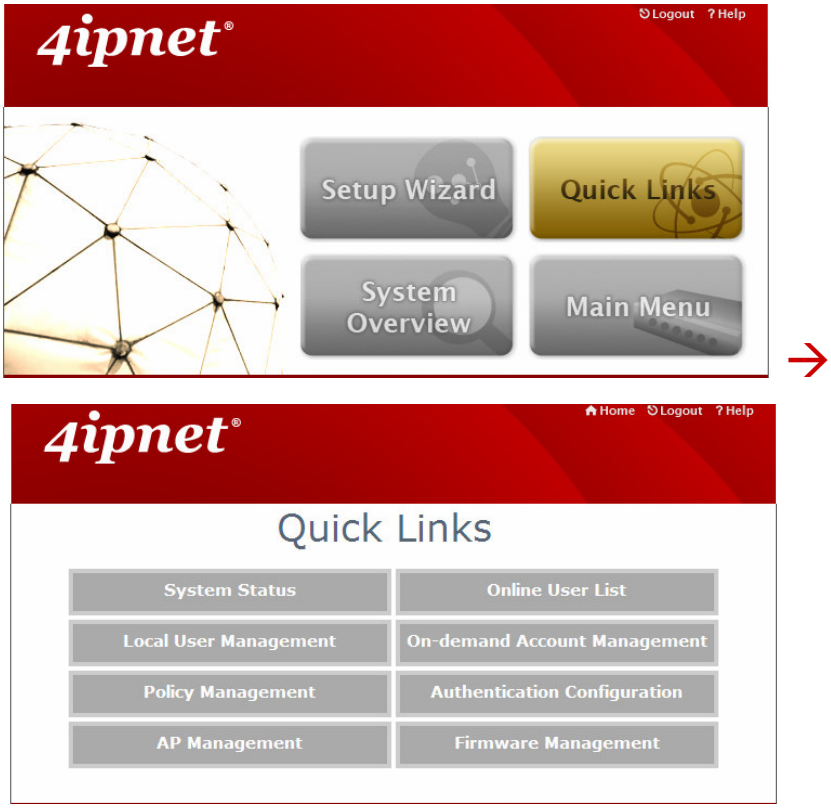
Step 4:

After a successful login, a "Home" page with four links called **Setup Wizard**, **Quick Links, System Overview**, and **Main Menu** will appear.

- **Setup Wizard:** Provide a four-step quick configuration of the system. Please refer to **Section 3.3.2. Setup Wizard** for more information.

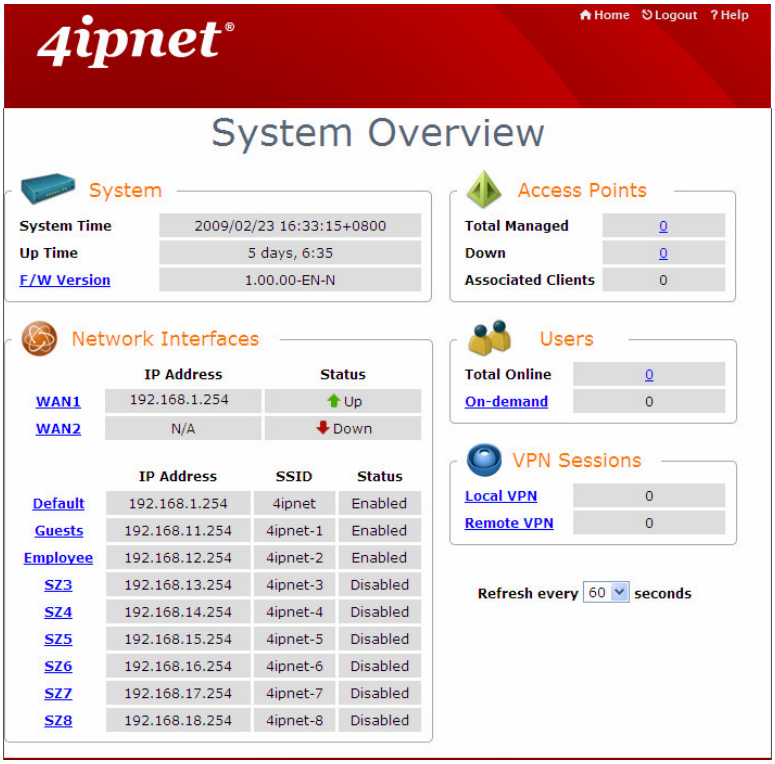
- **Quick Links:** Provide 8 links for the administrator to access frequently used pages of the web management interface directly, which are **System Status**, **Local User Management**, **Policy Management**, **Privilege List**, **Online User List**, **Guest Account Management**, **Authentication Configuration**, and **Firmware Management**.

© 2008 4IPNET, INC.



- **System Overview:** Provide an overview of the system status for the administrator. Certain hyperlinks of associated configuration pages are provided in this page for the administrator to access directly.

© 2008 4IPNET, INC.

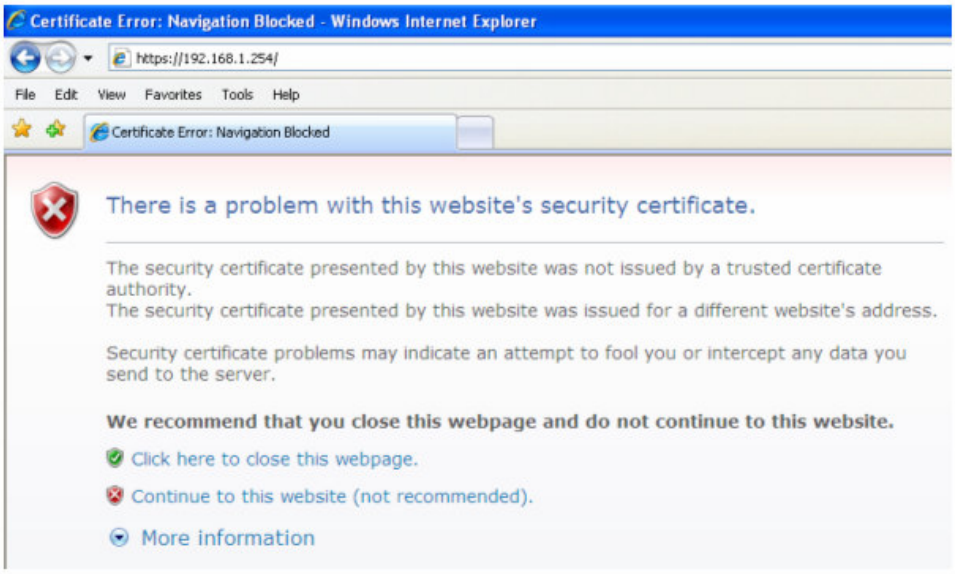


- **Main Menu:** Provide detailed configuration pages for administrators to configure the system manually. Please refer to **Section 4. Web Interface Configuration** for more information.

© 2008 4IPNET, INC.

Note: **Quick Links** and **System Overview** are not accessible until the system is configured via **Setup Wizard**.

For the first time, if WHG303 is not using a **trusted SSL certificate**, there will be a **"Certificate Error"**, because the browser treats WHG303 as an illegal website. Please press **"Continue to this website"** to continue. The default user login page will then appear in the browser. *For more information, please see **4.2.5 Additional Configuration***.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.1.254/
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

*If you can't get the login screen, the reasons may be: (1) The PC is set incorrectly so that the PC can't obtain the IP address automatically from the LAN port; (2) The IP address and the default gateway are not under the same network segment. Please use default IP address such as 192.168.1.xx in your network and then try it again. For the configuration on PC, please refer to **Appendix G. Network Configuration on PC & User Login.***

© 2008 4IPNET, INC.

After a successful login to WHG303, a web management interface with a welcome message will appear.

4ipnet
Home
Logout
Help
System
Users
Access Points
Network
Utilities
Status
Welcome to System Main Menu
This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.
Functions are separated into 6 main categories:
System , Users , Access Points , Network , Utilities and Status.
Copyright © 2009 4IPNET, INC. All rights reserved.

Note: To logout, simply click the ***Logout*** icon on the upper right corner of the interface to return to the login screen.

© 2008 4IPNET, INC.

3.3.2 Setup Wizard

WHG303 provides a **Setup Wizard** for quick configuration. The **Setup Wizard** comprises of four basic steps. Follow the instructions of Setup Wizard to enter the required information step by step, save your settings, and restart WHG303. Then, the system is ready to use. The four steps of Configuration Wizard are listed below:

Step I. General

Step 2. WAN1 Interface

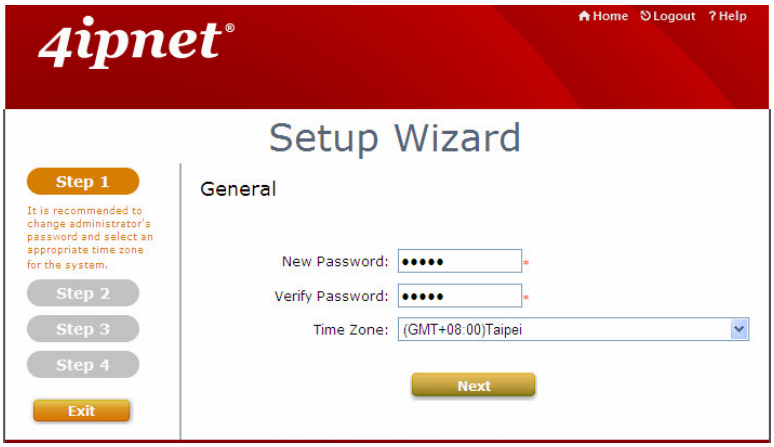
Step 3. Local User Account (Optional)

Step 4. Confirm and Restart

Please follow the steps below to complete the Setup Wizard configuration.

Step 1: General

- Click the ***Setup Wizard*** in the **Home** page to start the configuration process.
- Enter a new password in the *New Password* field, and re-enter it again in the *Verify Password* field (a maximum of 20 characters and no spaces allowed in between).
- Select an appropriate time zone from the *Time Zone* drop-down list box to set up the system time.
- Click ***Next*** to continue.



For security concern, it is strongly recommended to change the administrator's password.

© 2008 4IPNET, INC.

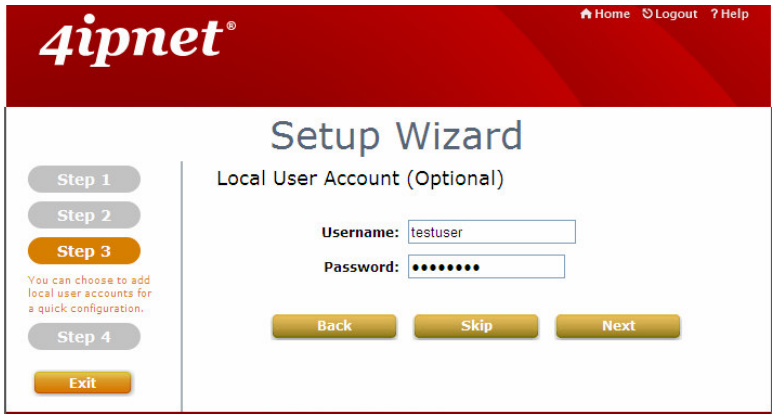
Step 2: WAN1 Interface and Wireless

- Select a proper type of Internet connection for WAN1 interface from the following three available connections: **Static**, **Dynamic**, or **PPPoE**. Your ISP or network administrator can advise on the connection type available to you. Below depicts an example for **Dynamic**.
- Click ***Next*** to continue.

Step 3: Local User Account (Optional)

New local accounts can be created and added into the database via this optional function. If local user accounts are not required, click ***Skip*** to go directly to **Step 4**. However, it is recommended to create at least one local user account in order to verify the system's readiness upon completion of this **Setup Wizard**.

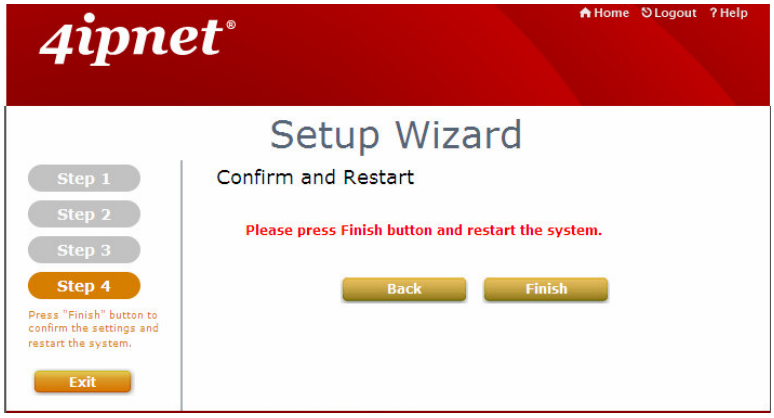
- Enter the *Username* (e.g. **"testuser"**) and *Password* (e.g. **"testuser"**) to create a new local account.
- Click ***Next*** to continue.
- More local accounts can be added by clicking the ***Back*** button in **Step 4**.



Step 4: Confirm and Restart

- Click ***Finish*** to save current settings and restart the system.

© 2008 4IPNET, INC.



- A confirmation dialog box will then appear. Click ***OK*** to continue.

- A **Confirm and Restart** message will appear on the screen during the restarting process. Please do not interrupt the system until the Administrator Login Page appears.

Note: The system is trying to locate a DNS server at this stage. Therefore, a longer startup time is required if the configured DNS cannot be found.

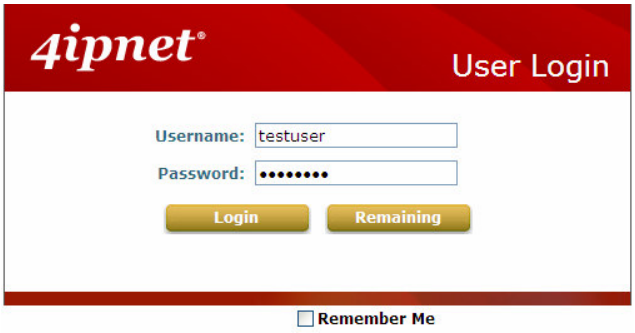
- When the following Administrator Login Page appears, it means the restart process is now completed.

© 2008 4IPNET, INC.

3.3.3 User Login Portal Page

In order to be granted network access via WHG303's, a user must be authenticated first by entering a correct username and password on the User Login Portal Page. To verify whether the configuration of the new local user account(s) created via the **Setup Wizard** has been completed successfully:

1. Connect a client device (e.g. laptop, PC) to the LAN1 Port of WHG303. The device will obtain an IP address automatically via DHCP.
2. Open a web browser on a client device, access any URL, and then the default **User Login Page** will appear.
3. Enter the *Username* and *Password* of a local user account previously generated via Setup Wizard (e.g. **"testuser@local"** as the *Username* and **"testuser"** as the *Password*); then Click ***Login.***

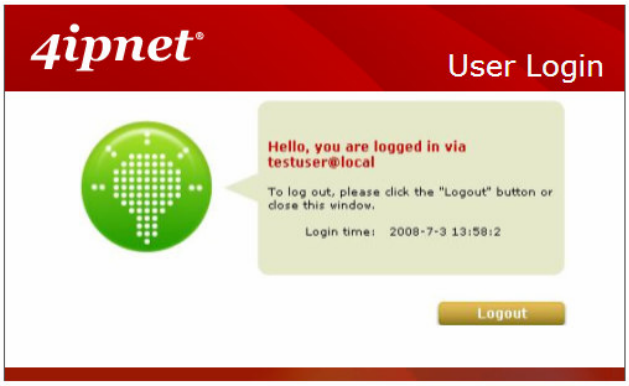


Note:

1. WHG303 supports multiple authentication options including built-in local user database and external authentication database (e.g. RADIUS). The system will automatically identify which authentication option is used from the full username entered.
2. The format of a full (valid) username is **userid@postfix,** where **"userid"** is the user ID and **"postfix"** is the name of the selected authentication option.
3. **Exception:** The postfix can be omitted only when the default authentication option is used. For example, **"LOCAL"** is the default authentication option at this system; therefore, you may enter either **"testuser"** or **"testuser@local"** in the *Username* field.

Congratulation!

The Login Success Page will appear after a client has successfully logged into WHG303 and has been authenticated by the system. The appearance of Login Success Page means that WHG303 has been installed and configured properly.


4ipnet
User Login
Hello, you are logged in via testuser@local
To log out, please click the "Logout" button or close this window.
Login time: 2008-7-3 13:58:2
Logout

© 2008 4IPNET, INC.

4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of 4ipnet WHG303.

4ipnet
Home
Logout
Help
System
Users
Access Points
Network
Utilities
Status
Welcome to System Main Menu
This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.
Functions are separated into 6 main categories:
System , Users , Access Points , Network , Utilities and Status.
Copyright © 2009 4IPNET, INC. All rights reserved.

© 2008 4IPNET, INC.

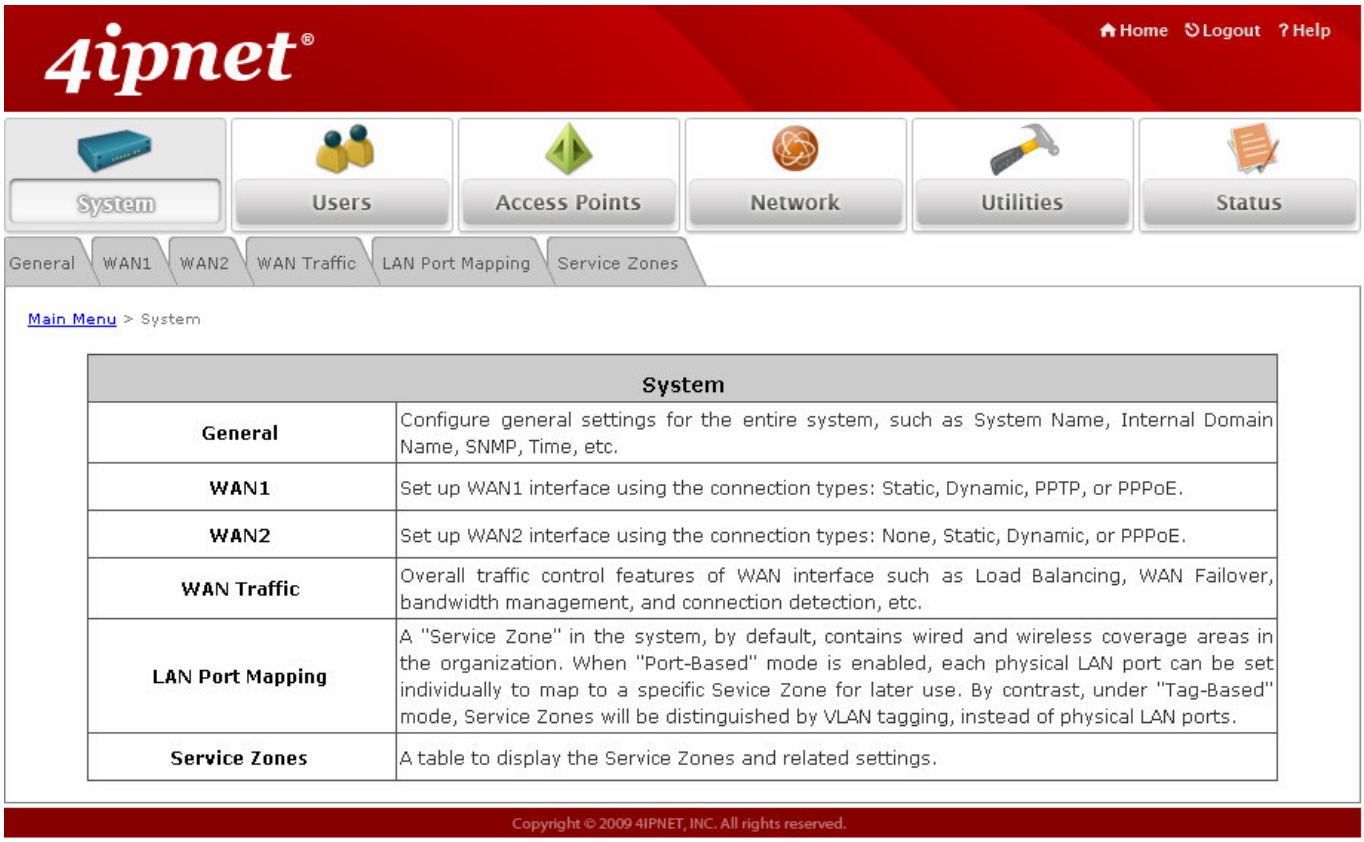
OPTION	System	Users	Access Points	Network	Utilities	Status
FUNCTION	General	Authentication	List	NAT	Password Change	System
	WAN 1	Black List	Discovery	Privilege	Backup & Restore	Interface
	WAN 2	Group	Adding	Monitor IP	System Upgrade	Routing Table
	WAN Traffic	Policy	Templates	Walled Garden	Restart	Online Users
	LAN Port Mapping	Additional Control	Firmware	Walled Garden AD List	Network Utilities	User Logs
	Service Zones		Upgrade	Proxy Server		E-mail & SYSLOG
			WDS Management	DDNS		
				Client Mobility		
				VPN		

*After finishing the configuration of the settings, please click **Apply** and pay attention to see if a RESTART message appears on the screen. If such message appears, the system must be restarted to allow the new settings to take effect. All on-line users will be disconnected during restart.*

© 2008 4IPNET, INC.

4.1 System Configuration

This section includes the following functions: **General**, **WAN1 Configuration**, **WAN2 Configuration**, **WAN Traffic Settings**, **LAN Port Mapping** and **Service Zones**.

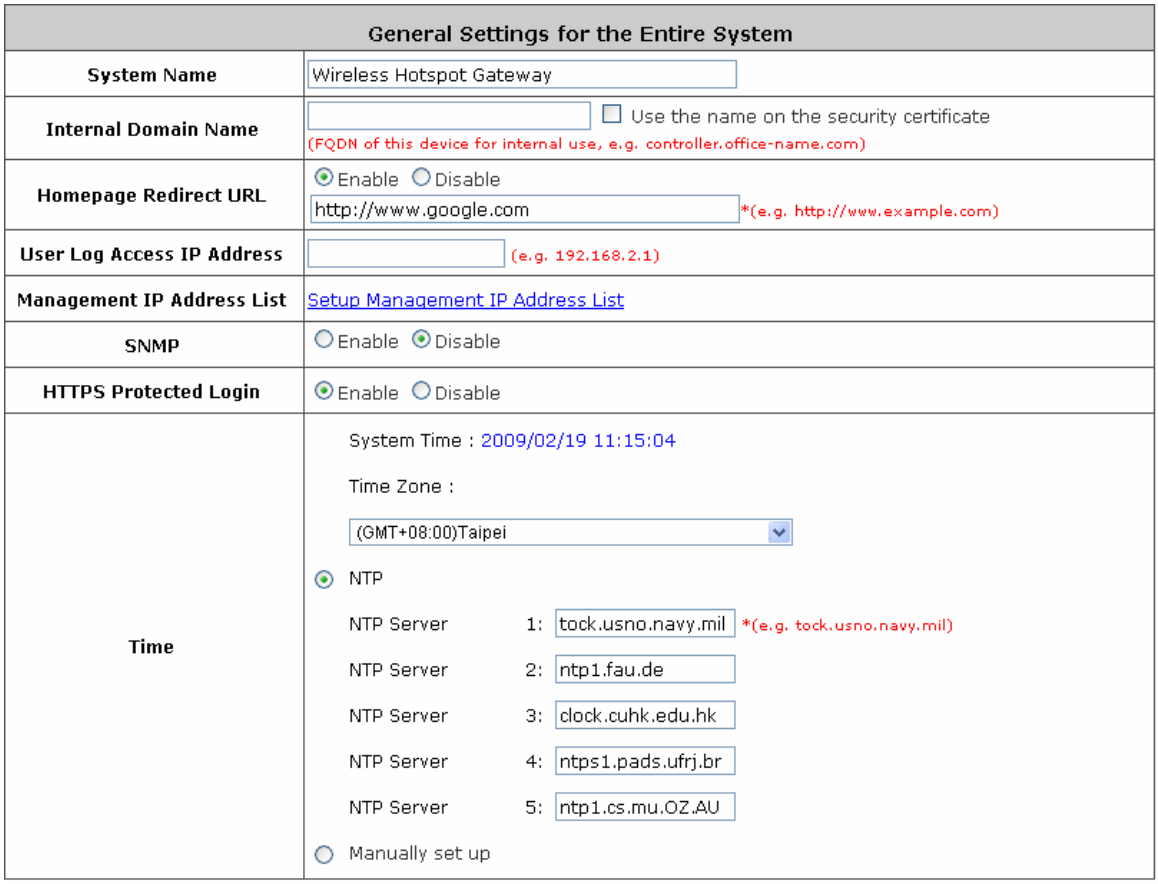


System	
General	Configure general settings for the entire system, such as System Name, Internal Domain Name, SNMP, Time, etc.
WAN1	Set up WAN1 interface using the connection types: Static, Dynamic, PPTP, or PPPoE.
WAN2	Set up WAN2 interface using the connection types: None, Static, Dynamic, or PPPoE.
WAN Traffic	Overall traffic control features of WAN interface such as Load Balancing, WAN Failover, bandwidth management, and connection detection, etc.
LAN Port Mapping	A "Service Zone" in the system, by default, contains wired and wireless coverage areas in the organization. When "Port-Based" mode is enabled, each physical LAN port can be set individually to map to a specific Sevice Zone for later use. By contrast, under "Tag-Based" mode, Service Zones will be distinguished by VLAN tagging, instead of physical LAN ports.
Service Zones	A table to display the Service Zones and related settings.

© 2008 4IPNET, INC.

4.1.1 General

Main information about 4ipnet WHG303 is shown as follows:

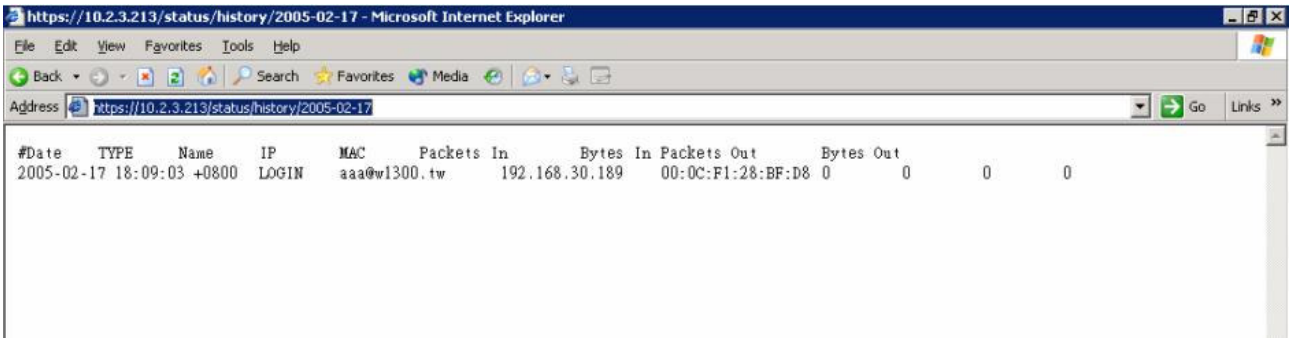


- **System Name:** Set the system's name or use the default.
- **Device Name:** FQDN (Fully-Qualified Domain Name). This is the domain name of the WHG303 as seen on client machines connected on LAN ports. A user on client machine can use this domain name to access WHG303 instead of its IP address. In addition, when "***Use the name on the security certificate***" option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.
- **Home Page:** Enter the URL of a Web server as the homepage. Once logged in successfully, users will be directed to this homepage, such as http://www.4ipnet.com, regardless of the original homepage set in their computers.

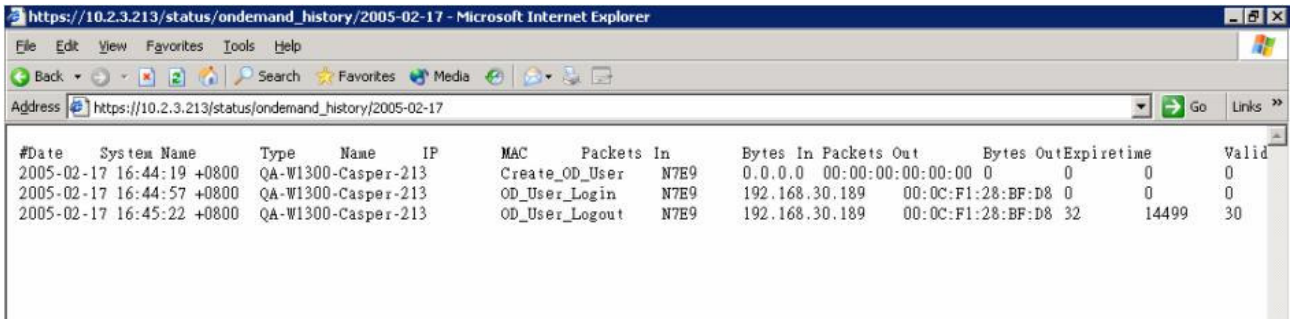
© 2008 4IPNET, INC.

- **User Log Access IP Address:** Specify an IP address of the administrator's computer or a billing system to get access history information of WHG303 with the predefined URLs. An example is provided as follows:

  Traffic History：https://10.2.3.213/status/history/2005-02-17


https://10.2.3.213/status/history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/history/2005-02-17
Go Links
#Date TYPE Name IP MAC Packets In Bytes In Packets Out Bytes Out
2005-02-17 18:09:03 +0800 LOGIN aaa@wl300.tw 192.168.30.189 00:0C:F1:28:BF:D8 0 0 0 0

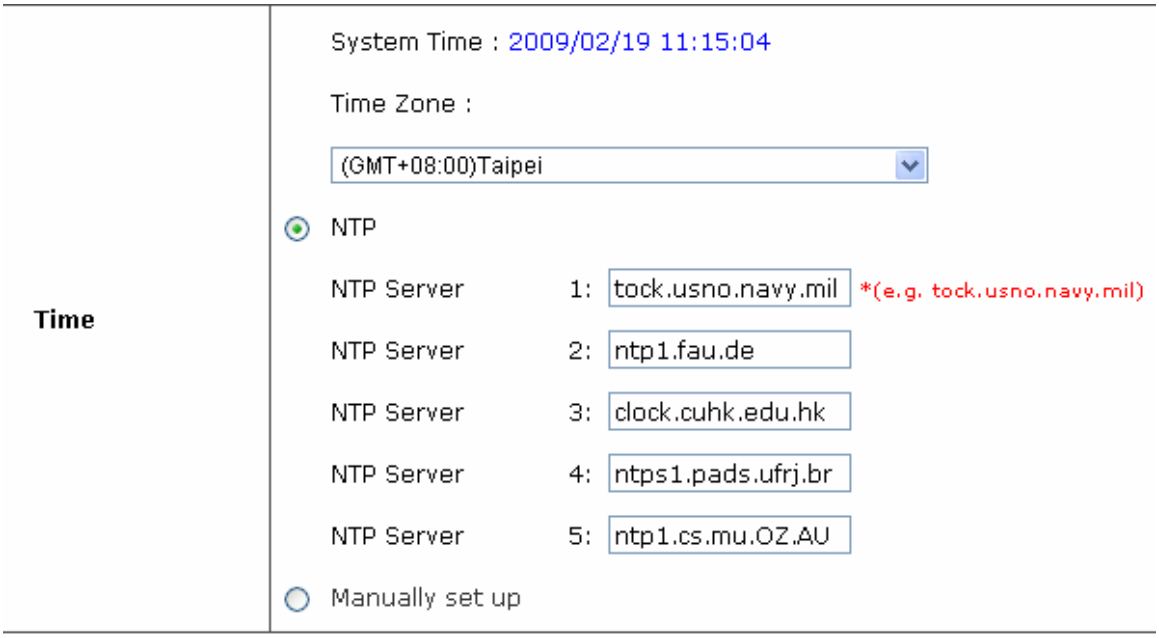
  On-demand History：https://10.2.3.213/status/ondemand_history/2005-02-17


https://10.2.3.213/status/ondemand_history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/ondemand_history/2005-02-17
Go Links
#Date System Name Type Name IP MAC Packets In Bytes In Packets Out Bytes Out Expiretime Valid
2005-02-17 16:44:19 +0800 QA-W1300-Casper-213 Create_OD_User N7E9 0.0.0.0 00:00:00:00:00:00 0 0 0 0
2005-02-17 16:44:57 +0800 QA-W1300-Casper-213 OD_User_Login N7E9 192.168.30.189 00:0C:F1:28:BF:D8 0 0 0
2005-02-17 16:45:22 +0800 QA-W1300-Casper-213 OD_User_Logout N7E9 192.168.30.189 00:0C:F1:28:BF:D8 32 14499 30

- **Management IP Address List:** The IP address or subnet of remote management PCs. Only PCs within this IP range on the list are allowed to access the system's web management interface. For example, 10.2.3.0/24 means that as long as an administrator is using a computer with the IP address range of 10.2.3.0/24, he or she can access the web management page. Another example is 10.0.0.3: if an administrator is using a computer with the IP address of 10.0.0.3, he or she can access the web management page.
- **SNMP:** If this function is enabled, the Manager IP and the community can be assigned to access the Management Information Base (MIB) of the system.
- **User logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.

© 2008 4IPNET, INC.

- **Time:** NTP (Network Time Protocol) communication protocol can be used to synchronize the system time with remote time server. Please specify the local time zone and the IP address of at least one NTP server for adjusting the time automatically (Universal Time is Greenwich Mean Time, GMT). The time can also be manually configured by selecting **"Set Device Date and Time"** and then entering the date and time in these fields.



© 2008 4IPNET, INC.

4.1.2 WAN1 Configuration

There are 4 connection types for the WAN1 Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.

- **Static IP Address:** Manually specifying the IP address of the WAN Port. The fields with red asterisks are required to be filled in.

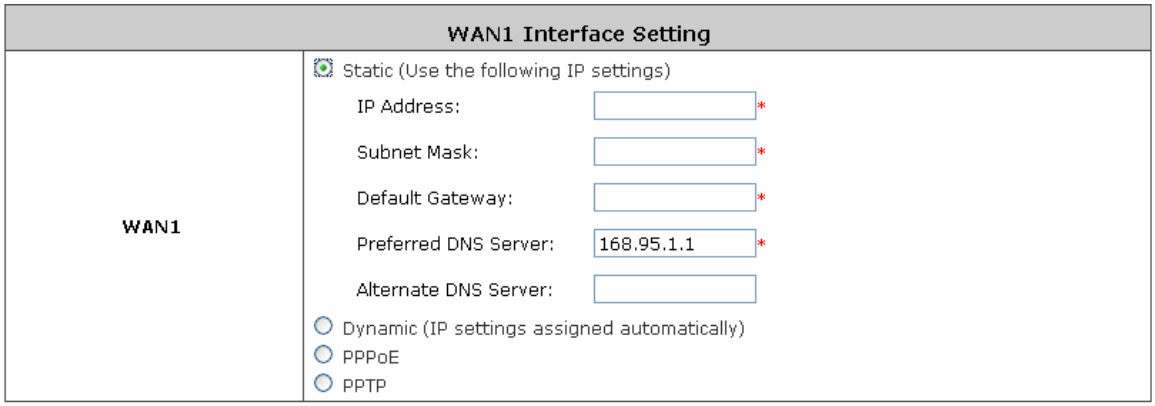
  IP Address: The IP address of the WAN1 port.

  Subnet Mask: The subnet mask of the WAN1 port.

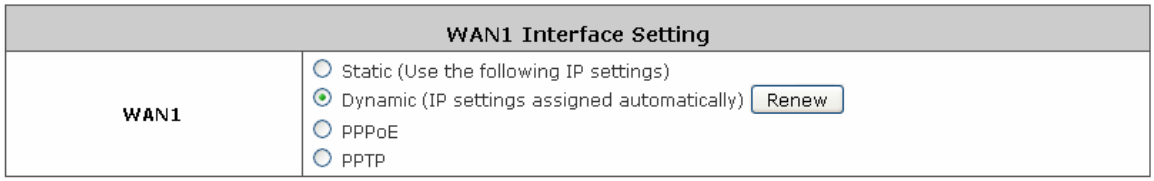
  Default Gateway: The gateway of the WAN1 port.

  Preferred DNS Server: The primary DNS server used by the system.

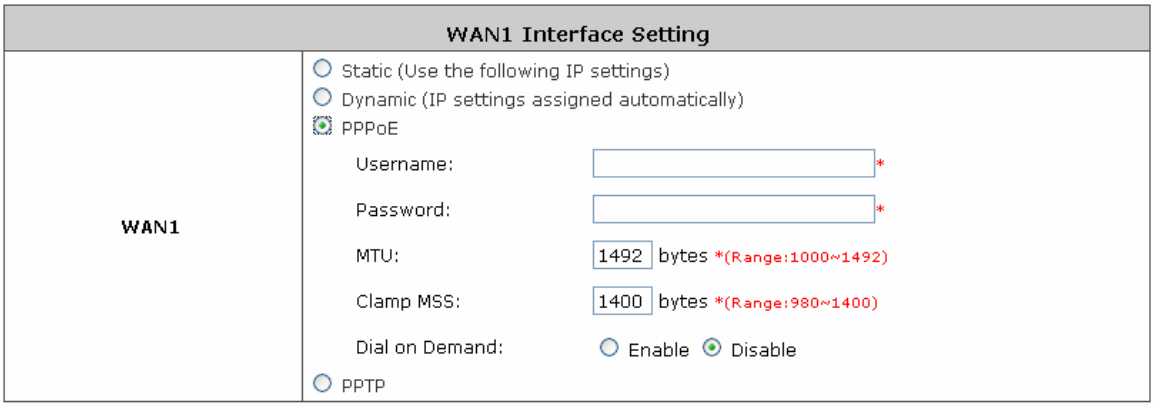
  Alternate DNS Server: The substitute DNS server used by the system. This is an optional field.



- **Dynamic IP Address:** It is only applicable for the network environment where the DHCP server is available on the network. Click the ***Renew*** button to get an IP address automatically.

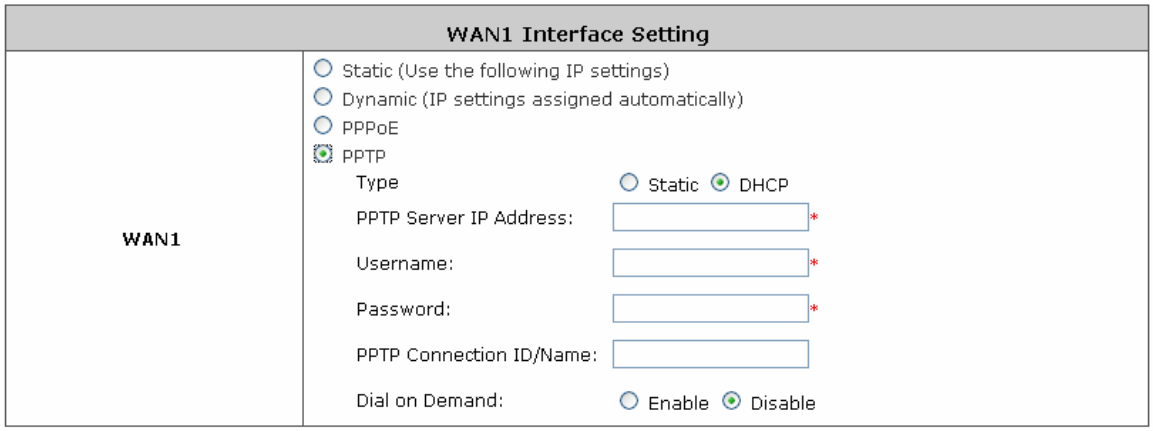


- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"User Name"**, **"Password"**, **"MTU"** and **"CLAMPMSS"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



© 2008 4IPNET, INC.

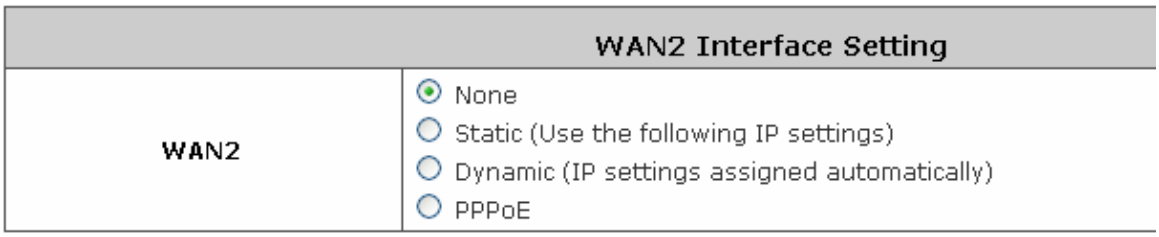
- **PPTP Client:** Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



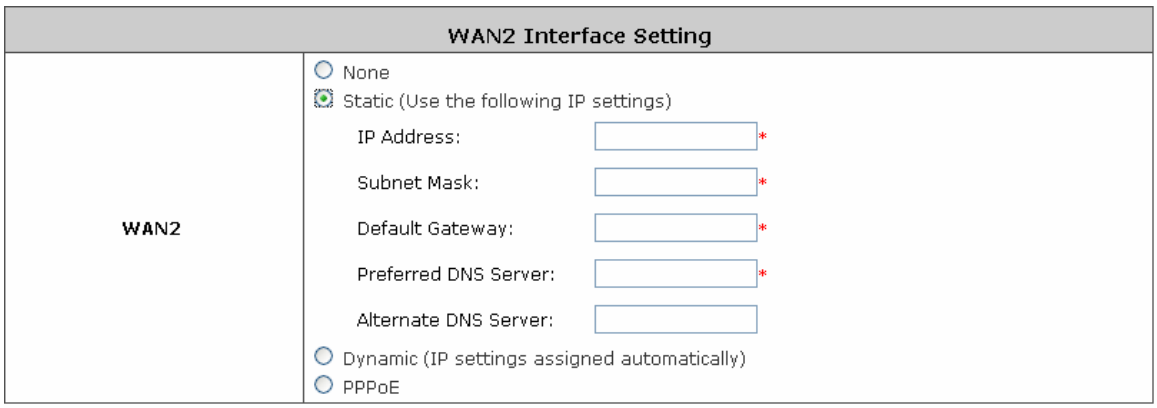
© 2008 4IPNET, INC.

4.1.3 WAN2 Configuration

Select **None** to disable this WAN2 interface, or there are 3 connection types for the WAN2 port: **Static IP Address, Dynamic IP Address,** and **PPPoE Client**.



- **None**: The WAN2 Port is disabled.
- **Static IP Address:** Manually specifying the IP address of the WAN port. The red asterisks indicate required fields to be filled in.



IP address: the IP address of the WAN2 port.

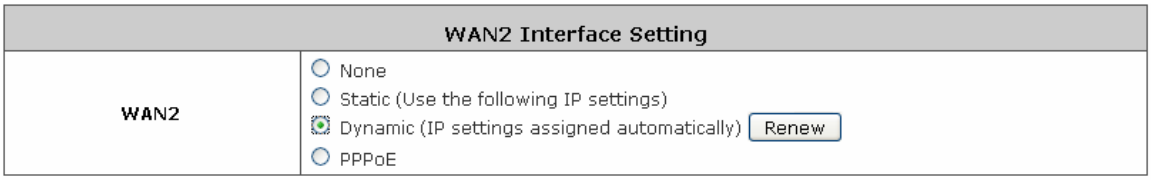
Subnet mask: the subnet mask of the network WAN2 port connects to.

Default gateway: a gateway of the network WAN2 port connects to.

Preferred DNS Server: The primary DNS server used by the system.

Alternate DNS Server: The substitute DNS server used by the system. This is an optional field.

- **Dynamic IP address:** It is only applicable for the network environment where a DHCP server is available. Click the ***Renew*** button to get an IP address.



- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"User Name"** and **"Password"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, **Maximum Idle Time can be set**. When the idle time is reached, the system will automatically disconnect itself.

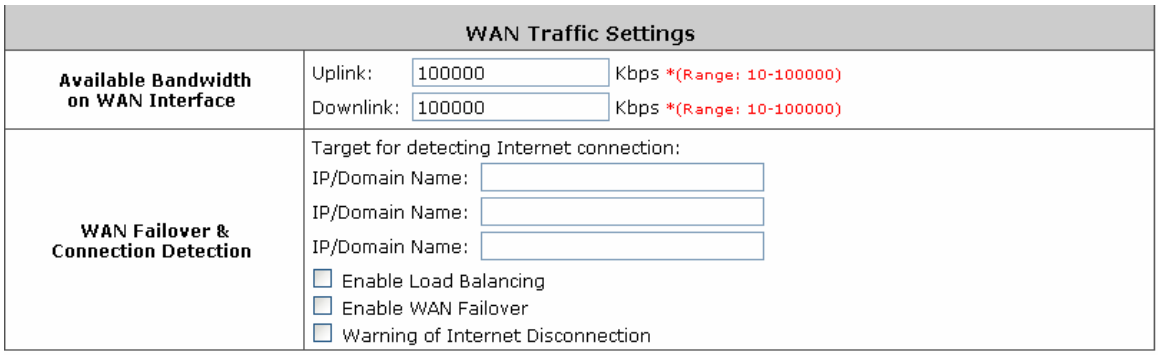
© 2008 4IPNET, INC.

WAN2 Interface Setting	
WAN2	None Static (Use the following IP settings) Dynamic (IP settings assigned automatically) PPPoE Username: * Password: * MTU: 1492 bytes *(range:1000~1492) Clamp MSS: 1400 bytes *(range:980~1400) Dial on Demand: Enabled Disabled

© 2008 4IPNET, INC.

4.1.4 WAN Traffic Settings

The section is for administrators to configure the control over the entire system's traffic though the WAN interface (WAN1 and WAN2 ports).



Available Bandwidth on WAN Interface:

- **Uplink:** It specifies the maximum uplink bandwidth that can be shared by clients of the system.
- **Downlink:** It specifies the maximum downlink bandwidth that can be shared by clients of the system.

WAN Failover & Connection Detection &:

- **Target for detecting Internet connection:** These URLs are used by the system as the targets to detect Internet connection, for alerting Internet disconnection and WAN Failover. At least one URL is required to enable WAN Failover.
- **Enable Load Balancing:** Outbound load balancing is supported by the system. When enabled, the system will allocate traffic between WAN1 and WAN2 dynamically according to designed algorithms based on the weight ratio.
  - **WAN1 Weight:** The percentage of traffic through WAN1. (Range: 1~99; by default, it is 50)
  - **Base:** The weight ratio between WAN1 and WAN2 can be based on Sessions, Packets or Bytes. Packets and Bytes are based on historic data. New connection sessions will be distributed between WAN1 and WAN2 by a weight ratio using random number.
- **Enable WAN Failover:** Normally a Service Zone uses WAN1 as it primary WAN interface. When enabled and WAN2 is available, WAN1's traffic will be routed to WAN2 when WAN1 connection is down. On the other hand, a Service Zone's policy could also use WAN2 as its interface; in that case, if WAN2 is down, the WAN2's traffic under its policy will also be routed to WAN1.
  - **Fall back to WAN1 when WAN1 is available again:** If WAN Failover is enabled, the traffic will be routed to WAN2 automatically when WAN1 connection fails. When **fall back to WAN1** is enabled, the routed traffic will be connected back to WAN1 when WAN1 connection is recovered.
- **Warning of Internet Disconnection:** When enabled, there is a text box available for the administrator to enter a reminding message. This reminding message will appear on clients' screens when Internet connection is down.

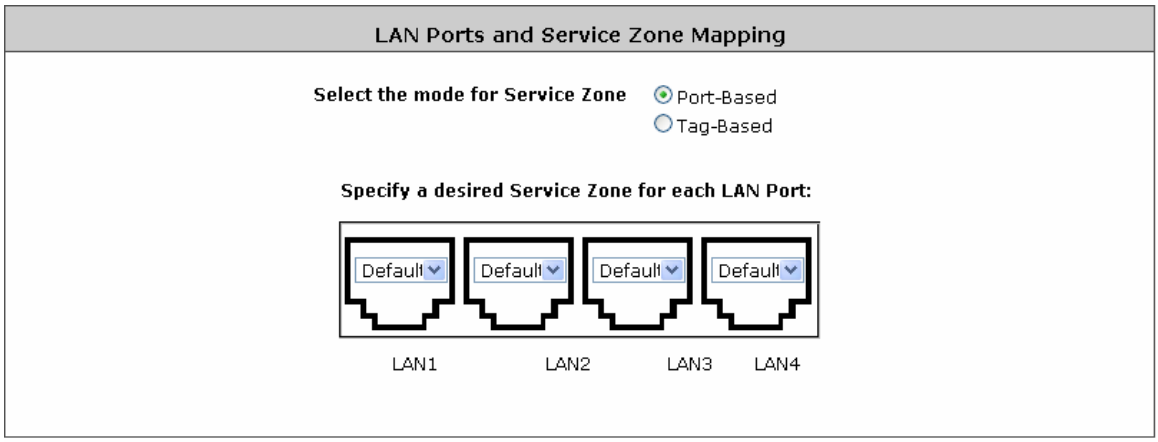
© 2008 4IPNET, INC.

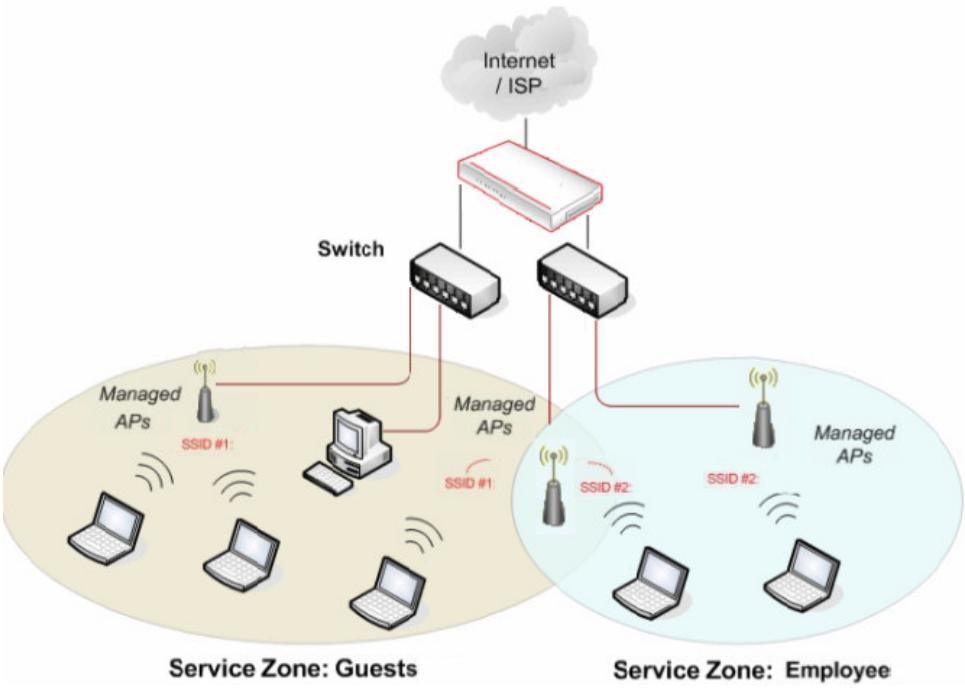
SIP authentication is exempt from Load Balancing and WAN Failover. A fixed WAN port is used for SIP traffic.

© 2008 4IPNET, INC.

4.1.5 LAN Port Mapping

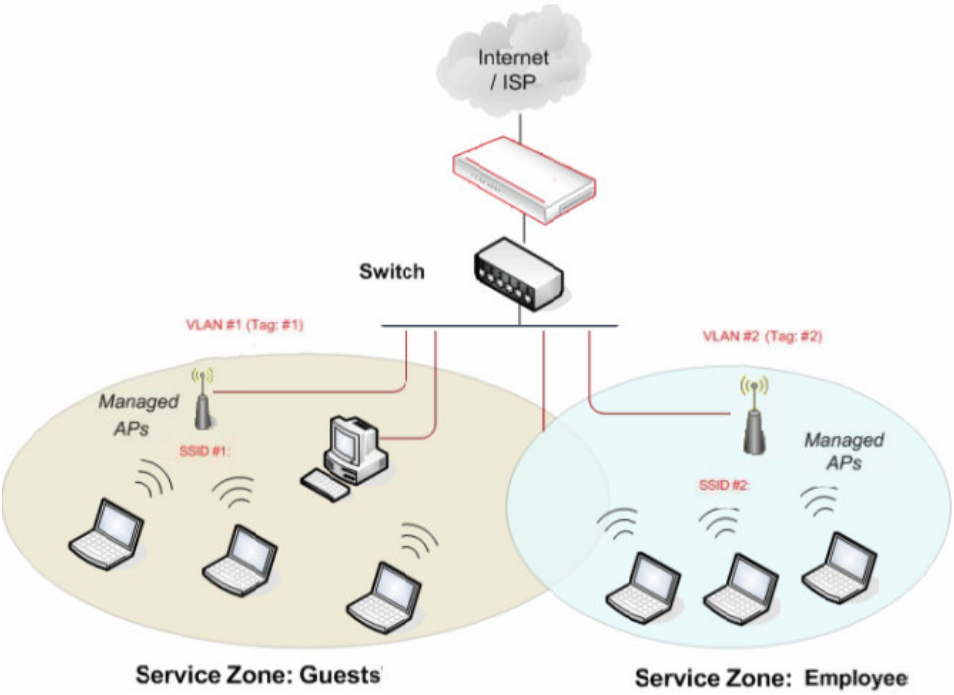
WHG303 supports multiple Service Zones in either of the two VLAN modes, **Port-Based** or **Tag-Based**, but not concurrently. In **Port-Base** mode, each LAN port can only serve traffic from one Service Zone as each Service Zone is identified by physical LAN ports. In **Tag-Based** mode, each LAN port can serve traffic from any Service Zone as each Service Zone is identified by VLAN tags carried within message frames. **By default, the system is in Port-Based mode with Default Service Zone enabled and all LAN ports are mapped to Default Service Zone.** Compare the two figures below to see the differences.





【Port-Based】

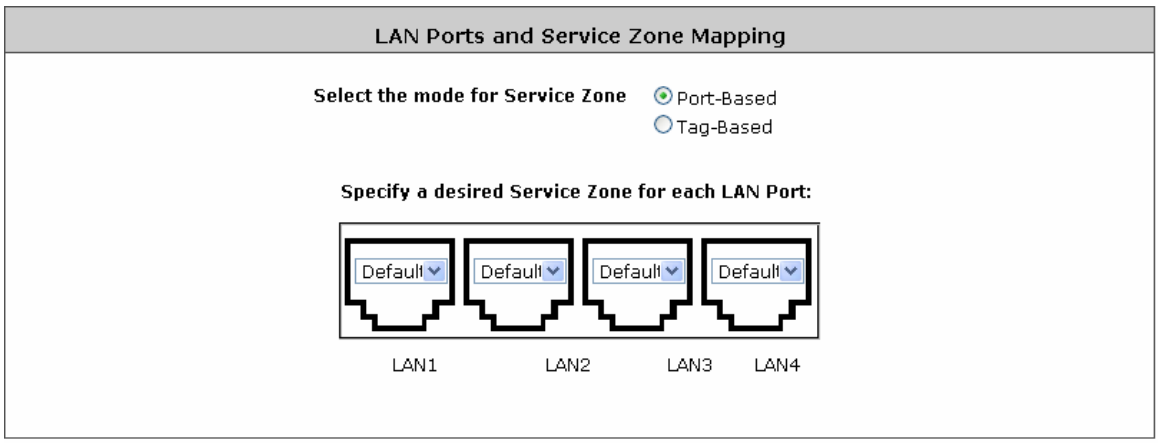
© 2008 4IPNET, INC.



【Tag-Based】

It is recommended that the administrator decides which mode is better for a multiple-service-zone deployment before proceeding further with the system configuration. Settings for the two VLAN modes are slightly different, for example, the VLAN Tag setting is required for Tag-Based mode.

- **Select Service Zone Mode**: Select a VLAN mode, either ***Port-Based*** or ***Tag-Based***.



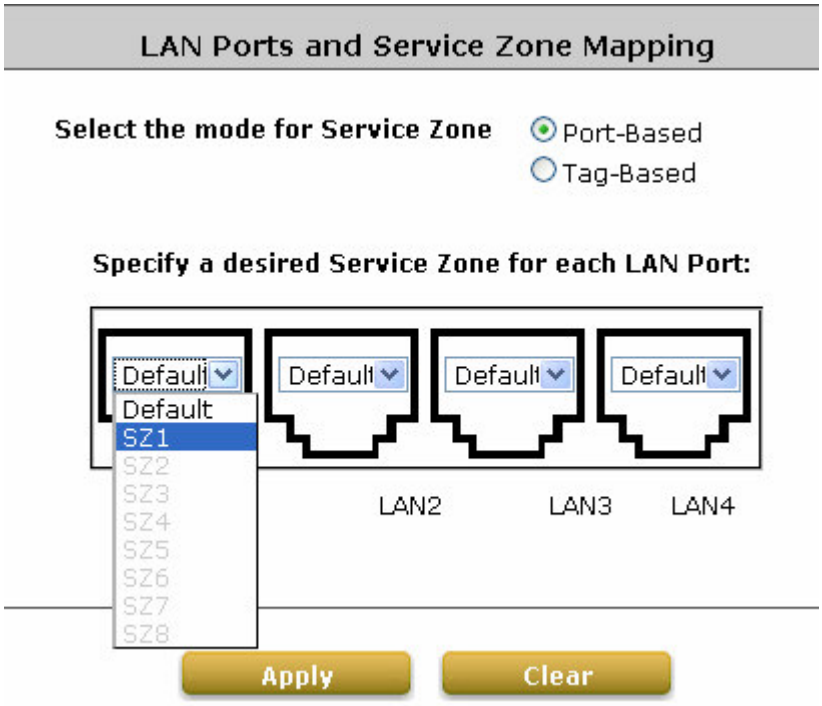
The switches deployed under WHG303 in Port-Based mode must be Layer2 Switches only. The switch deployed under WHG303 in Tag-Based mode must be a VLAN switch only.

- **Port-Based:** When Port-Based mode is selected, traffic from different virtual Service Zones will be distinguished by physical LAN ports. Each LAN port can be mapped to a Service Zone in the form of a

© 2008 4IPNET, INC.

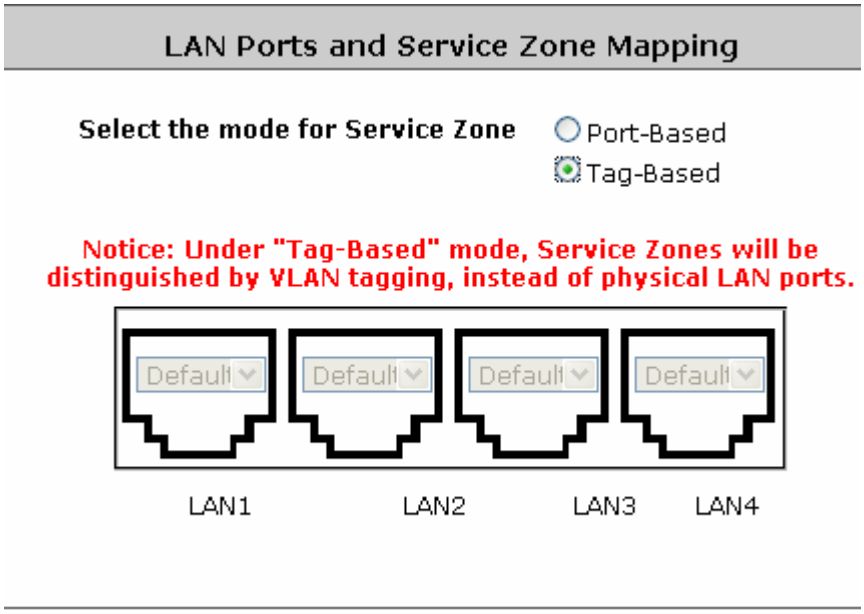
many-to-one mapping between ports and Service Zones.

- **Specify a desired Service Zone for each LAN Port:** For each LAN port, select a Service Zone to which the LAN port is to be mapped from the drop-down list box.
  By factory default, all LAN ports are mapped to Default Service Zone; therefore, the administrator can enter the web management interface via any LAN port upon the first power up of the system. From the drop-down list box, all disabled Service Zones are gray-out; to activate any desired Service Zone, please configure the desired Service Zone under the **Service Zone** tab and enable its *Service Zone Status* (refer to **4.1.7. Service Zones**).



- **Tag-Based:** When the Tag-Based mode is selected, traffic from different virtual Service Zones will be distinguished by VLAN tagging, instead of by physical LAN ports.
  Select *Tag-Based* and then click ***Apply*** to activate the Tag-Based VLAN function. When a restart message screen appears, do NOT restart the system until you have completed the configuration under the **Service Zones** tab first.

© 2008 4IPNET, INC.



Note: For more information on enabling and configuring Service Zones, please refer to **Appendix D. Service Zone Deployment Example.**

© 2008 4IPNET, INC.

4.1.6 Service Zones

A *Service Zone* is a logical network area to cover certain wired and wireless networks in an organization such as SMB or branch offices. By associating a unique VLAN Tag and SSID with a Service Zone, administrators can separate wired network and wireless network into different logical zones. Users attempting to access the resources within the Service Zone will be controlled based on the access control profile of the Service Zone, such as authentication, security feature, wireless encryption method, traffic control, and etc.

There are up to nine Service Zones to be utilized; by default, they are named as: **Default**, **SZ1~SZ8**, as shown in the table below.

Service Zone Settings

Service Zone Name	LAN Port Mapping	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default		4ipnet	None	Policy 1	Server 1	Enabled	Configure
SZ1		4ipnet-1	None	Policy 1	Server 1	Disabled	Configure
SZ2		4ipnet-2	None	Policy 1	Server 1	Disabled	Configure
SZ3		4ipnet-3	None	Policy 1	Server 1	Disabled	Configure
SZ4		4ipnet-4	None	Policy 1	Server 1	Disabled	Configure
SZ5		4ipnet-5	None	Policy 1	Server 1	Disabled	Configure
SZ6		4ipnet-6	None	Policy 1	Server 1	Disabled	Configure
SZ7		4ipnet-7	None	Policy 1	Server 1	Disabled	Configure
SZ8		4ipnet-8	None	Policy 1	Server 1	Disabled	Configure

【Port-Based】

© 2008 4IPNET, INC.

Service Zone Settings							
Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default	N/A	4ipnet	None	Policy 1	Server 1	Enabled	Configure
SZ1	1	4ipnet-1	None	Policy 1	Server 1	Disabled	Configure
SZ2	2	4ipnet-2	None	Policy 1	Server 1	Disabled	Configure
SZ3	3	4ipnet-3	None	Policy 1	Server 1	Disabled	Configure
SZ4	4	4ipnet-4	None	Policy 1	Server 1	Disabled	Configure
SZ5	5	4ipnet-5	None	Policy 1	Server 1	Disabled	Configure
SZ6	6	4ipnet-6	None	Policy 1	Server 1	Disabled	Configure
SZ7	7	4ipnet-7	None	Policy 1	Server 1	Disabled	Configure
SZ8	8	4ipnet-8	None	Policy 1	Server 1	Disabled	Configure

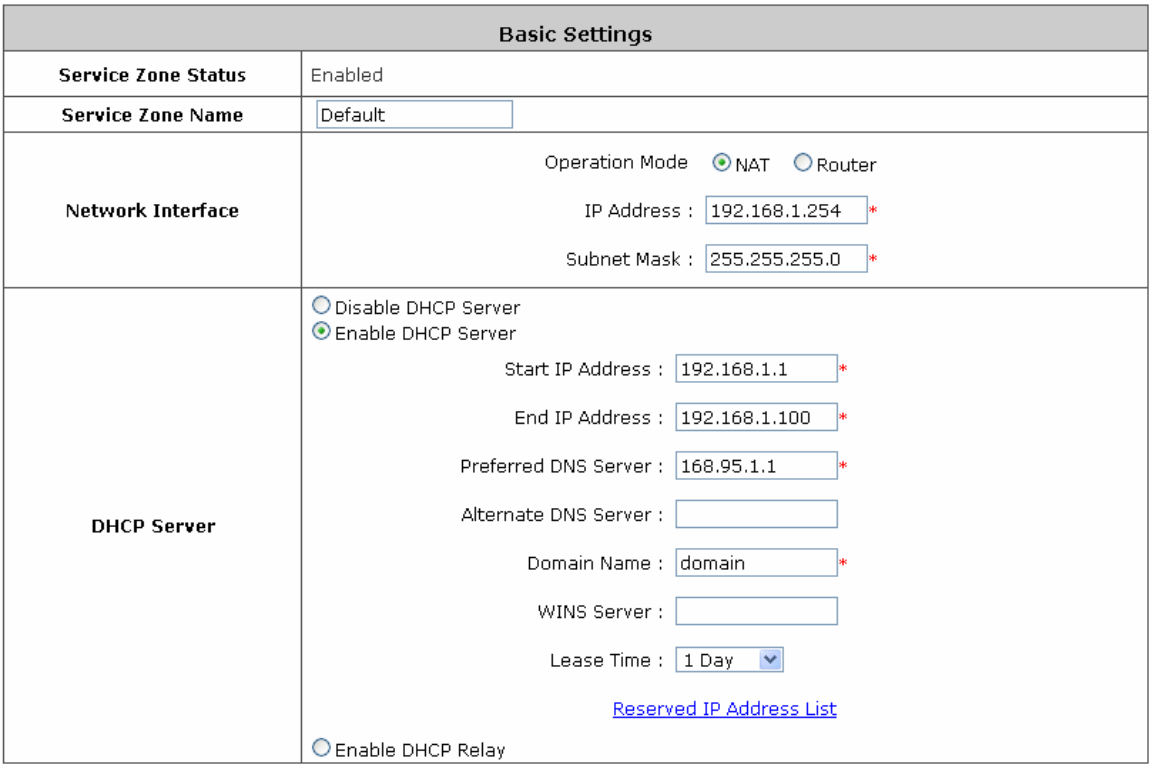
【Tag-Based】

- **Service Zone Name:** Mnemonic name of the Service Zone.
- **VLAN Tag:** The VLAN tag number that is mapped to the Service Zone.
- **SSID:** The SSID that is associated with the Service Zone.
- **WLAN Encryption:** Data encryption method for wireless networks within the Service Zone.
- **Applied Policy:** The policy that is applied to the Service Zone.
- **Default Authentication:** Default authentication method/server that is used within the Service Zone.
- **Status:** Each Service Zone can be enabled or disabled.
- **Details:** Configurable, detailed settings for each Service Zone.

Click ***Configure*** button to configure each Service Zone: **Basic Settings**, **SIP Interface Configuration**, **Authentication Settings**, **Wireless Settings**, and **Managed AP in Each Service Zone**.

1) Service Zone Settings – Basic Settings

© 2008 4IPNET, INC.



- **Service Zone Status:** Each service zone can be enabled or disabled except for the default service zone.
- **Service Zone Name:** The name of service zone could be input here.
- **Network Settings:**
  - **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
  - **IP address:** The IP Address of this service zone.
  - **Subnet Mask:** The subnet Mask of this service zone.
- **DHCP Server Settings:** Related information needed on setting up the DHCP Server is listed here. Please note that when "*Enable DHCP Relay"* is enabled, the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone.
  - **Start IP Address** / **End IP Address:** A range of IP addresses that built-in DHCP server will assign to clients. Note: please change the Management IP Address List accordingly (at *System Configuration >> System Information >> Management IP Address List*) to permit the administrator to access the WHG303 admin page after the default IP address of the network interface is changed.
  - **Preferred DNS Server:** The primary DNS server that is used by this Service Zone.
  - **Alternate DNS Server:** The substitute DNS server that is used by this Service Zone.
  - **Domain Name:** Enter the domain name for this service zone.
  - **WINS Server IP:** The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
  - **Lease Time:** This is the time period that the IP addresses issued from the DHCP server are valid and available.

© 2008 4IPNET, INC.

- **Reserved IP Address List:** Each service zone can reserve up to 40 IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with certain MAC address.

2) *Service Zone Settings – Assigned IP Address for AP Management*

Configure IP Range here by entering Start IP Address and End IP Addresse.

Assigned IP Address for AP Management	
IP Range	Start IP Address : 192.168.1.101 * End IP Address : 192.168.1.120 *

3) *Service Zone Settings – SIP Interface Configuration*

SIP Interface Configuration		
Enabled ☐	WAN Interface	WAN1

The system provides SIP proxy functionality, which allows SIP clients to pass through NAT. When enabled, all SIP traffic can pass through NAT via a fixed WAN interface. The policy route setting of SIP Authentication must be configured carefully because it must cooperate with the fixed WAN interface for SIP authentication.

SIP Transparent Proxy can be activated in both NAT and Router mode. SIP Authentication must support in either mode. For users logging in through SIP authentication, a policy can be chosen to govern SIP traffic. The policy's login schedule profile will be ignored for SIP authentication. Specific route and firewall rules of the chosen policy will be applied to SIP traffic.

© 2008 4IPNET, INC.

4) Service Zone Settings – Authentication Settings

Authentication Settings					
Authentication Required For the Zone	◉ Enabled ○ Disabled				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	◉	☑
	Server 2	POP3	pop3	○	☑
	Server 3	RADIUS	radius	○	☑
	Server 4	LDAP	ldap	○	☑
	On-demand User	ONDEMAND	ondemand	○	☑
	SIP	SIP	N/A	○	☐
Custom Pages	Login Page				Configure
	Logout Page				Configure
	Login Success Page				Configure
	Login Failed Page				Configure
	Login Success Page for On-demand User				Configure
	Logout Success Page				Configure
	Logout Failed Page				Configure
Group Permission for this Service Zone			Configure		
Default Policy in this Service Zone			Policy 1		Edit System Policies
Email Message for Login Reminding			◉ Enabled ○ Disabled		Edit Mail Message

- **Authentication Status:** When enabled, users must be authenticated before they get access to the network within this Service Zone.
- **Authentication Options:** There are total seven types of authentication database (LOCAL, POP3, RADIUS, LDAP, NTDOMAIN, ONDEMAND, and SIP) that are supported by the entire system. For each Service Zone, up to six authentication options can be enabled, and one of them can be set as the default option – so that users do not have to type in the postfix string while entering username during login.
- **Custom Pages:** Related login and logout pages can be customized by administrators for each service zone. Please refer to **Appendix J. Customizable Pages** for more details.
- **Group Permission for this Service Zone:**

  For each Service Zone, the administrator can set up multiple groups for that Service Zone. For each group, an associated policy can be assigned. Therefore, users in the same group follow the same policy and have the same privileges.

  To configure Group permission based on the role of this Service Zone.

  Click ***Configure*** to have further configuration or view the details.

  Click ***Enabled*** of the desired Group option(s) to allow the clients of the selected Group(s) to log into this Service Zone after a successful authentication. Moreover, a pre-defined Policy can be applied to any Group in this Service Zone.

© 2008 4IPNET, INC.

Click the hyperlink of the respective Group names in the **Edit Group Option** column to enter the **Group Configuration** tab, where zone permission and policy assignment can be further configured (refer to **4.2.3. Group Configuration**).

Group Permission Configuration & Policy Assignment - Service Zone : Default			
Group Option	**Enabled**	**Policy**	**To Zone Permission Configuration**
Group 1	☑	Policy 1	Group 1
Group 2	☑	Policy 2	Group 2
Group 3	☑	Policy 3	Group 3
Group 4	☑	Policy 4	Group 4
Group 5	☑	Policy 5	Group 5
Group 6	☑	Policy 6	Group 6
Group 7	☑	Policy 7	Group 7
Group 8	☑	Policy 8	Group 8

- **Default Policy in this Service Zone:** For each Service Zone, one policy can be applied to enforce the access control over the users. Please refer to **4.2.4 Policy Configuration** for complete description.
- **Email Message for Login Reminding:** When enabled, the system will automatically send an email to users if they attempt to send/receive their emails using POP3 email program (for example, Microsoft Outlook) before they are authenticated. Click ***Edit Mail Message*** to edit the message in HTML format:

5) *Service Zone Settings – Wireless Settings*

Wireless Settings		
SSID	4ipnet *	
Security	**Authentication**	Open System ☐ Enable 802.1X Authentication
	Encryption	None

- **Set SSID:** Each service zone can be mapped with its own SSID.
- **Access Point Security:** For each service zone, administrators can set up the wireless security profile, including **Authentication** and **Encryption**.

6) *Service Zone Settings – Managed AP in this Service Zone*

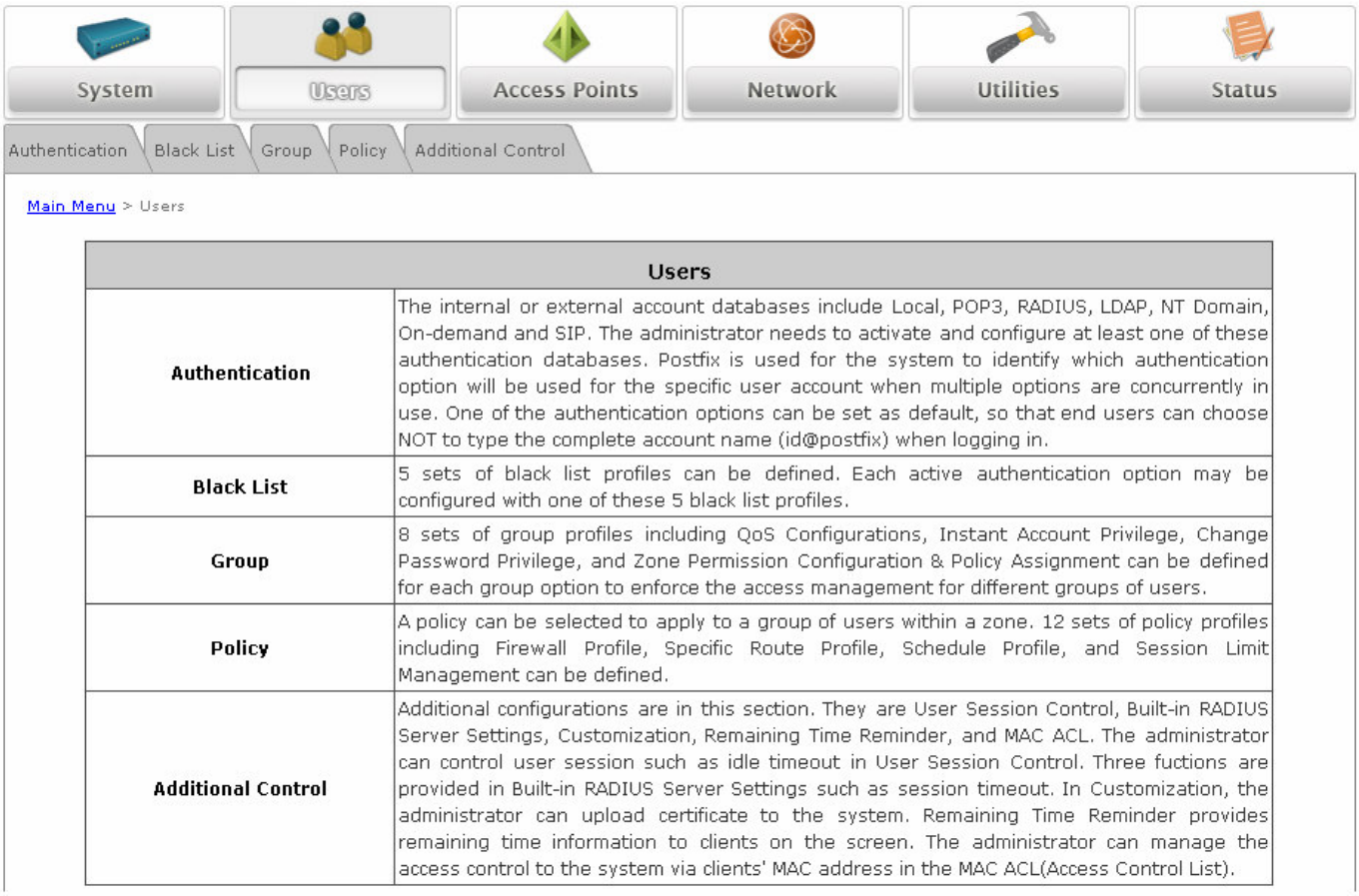
All managed APs that belong to this service zone are listed here.

Managed AP(s) in this Service Zone			
AP Type	**AP Name**	**IP Address** **MAC Address**	**Status**
EAP100	EAP100A	192.168.1.9 11:22:33:44:55:66	Offline

© 2008 4IPNET, INC.

4.2 User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Group Configuration**, **Policy Configuration** and **Additional Configuration**.



Users	
Authentication	The internal or external account databases include Local, POP3, RADIUS, LDAP, NT Domain, On-demand and SIP. The administrator needs to activate and configure at least one of these authentication databases. Postfix is used for the system to identify which authentication option will be used for the specific user account when multiple options are concurrently in use. One of the authentication options can be set as default, so that end users can choose NOT to type the complete account name (id@postfix) when logging in.
Black List	5 sets of black list profiles can be defined. Each active authentication option may be configured with one of these 5 black list profiles.
Group	8 sets of group profiles including QoS Configurations, Instant Account Privilege, Change Password Privilege, and Zone Permission Configuration & Policy Assignment can be defined for each group option to enforce the access management for different groups of users.
Policy	A policy can be selected to apply to a group of users within a zone. 12 sets of policy profiles including Firewall Profile, Specific Route Profile, Schedule Profile, and Session Limit Management can be defined.
Additional Control	Additional configurations are in this section. They are User Session Control, Built-in RADIUS Server Settings, Customization, Remaining Time Reminder, and MAC ACL. The administrator can control user session such as idle timeout in User Session Control. Three fuctions are provided in Built-in RADIUS Server Settings such as session timeout. In Customization, the administrator can upload certificate to the system. Remaining Time Reminder provides remaining time information to clients on the screen. The administrator can manage the access control to the system via clients' MAC address in the MAC ACL(Access Control List).

© 2008 4IPNET, INC.

4.2.1 Authentication Configuration

This section is for administrators to pre-configure authentication servers for the entire system's Service Zones. For a particular Service Zone, administrators can enable all the authentication servers which will be used and also specify a default authentication server in the page of *Service Zone Settings*. Concurrently up to four servers can be selected and pre-configured here by administrators from the five types of authentication databases (LOCAL, POP3, RADIUS, LDAP, and NTDOMAIN). In addition, there are two servers (On-demand User and SIP) that are selected by the system. For the Authentication Settings of each Service Zone, please see ***4.1.7 Service Zones***.

Authentication Settings			
Auth Option	**Auth Database**	**Postfix**	**Group**
Server 1	LOCAL	local	Group 1
Server 2	POP3	pop3	Group 1
Server 3	RADIUS	radius	Group 1
Server 4	LDAP	ldap	Group 1
On-demand User	ONDEMAND	ondemand	Group 1
SIP	SIP	N/A	None

- **Server Name:** There are several authentication options supported by WHG303: Server 1 to Server 4, On-demand User, and SIP. Click the hyperlink of the respective Server Name to configure the authentication server.
- **Auth Method:** There are different authentication methods in WHG303: **LOCAL**, **POP3**, **RADIUS**, **LDAP, NTDOMAIN**, **ONDEMAND** and **SIP**.
- **Postfix:** A postfix represents the authentication server in a complete username. For example, **user1@local** means that this user (user1) will be authenticated against the LOCAL authentication database.

Note: Concurrently only one server is allowed to be set as Local or NTDOMAIN authentication method.

- **Group:** An authentication option, such as POP3 or NT Domain, can be set as a Group with the same QoS or Privilege Profile setting.
  For more information on Group, please refer to **4.2.3. Group Configuration.**

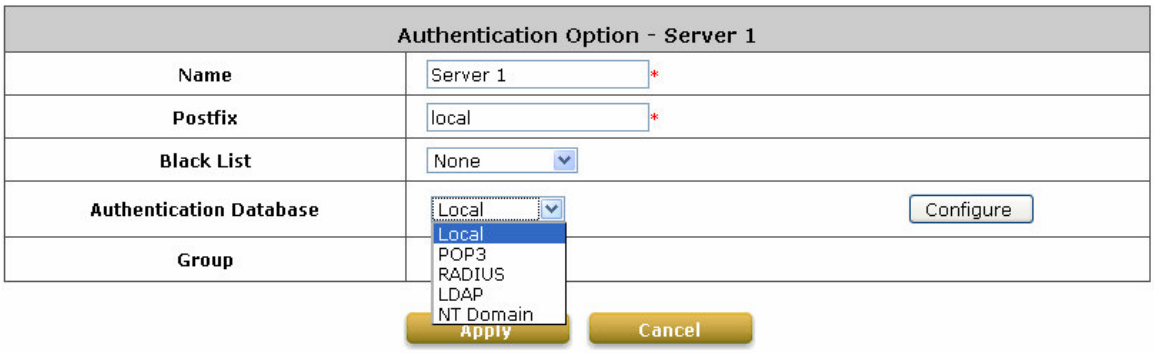
*After clicking **Apply**, there will be a restart message. You must click **Restart** to apply the settings.*

© 2008 4IPNET, INC.

- **Authentication Server Configuration**

  WHG303 provides four authentication servers and one on-demand server that the administrator can apply with different policy. Click on the server name to set the configuration for that particular server. After completing and clicking ***Apply*** to save the settings, go back to the previous page to select a server to be the default server and enable or disable any server on the list. Users can log into the default server without the postfix to allow faster login process.

  Server 1~4: There are 5 authentication methods, **Local User, POP3, RADIUS, LDAP** and **NTDomain,** to select from.



Server Name: Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_), space and dot (.) only. The length of this field is up to 40 characters. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.

Postfix: A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap". Set a postfix that is easy to distinguish (e.g. Local) and the server numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

The Policy Name cannot contain these words: MAC and IP.

Black List: There are 5 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one black list from the drop-down menu and this black list will be applied to this specific authentication option.

Group: Select one Group from the drop-down list box for this specific authentication option.

Authentication Method: Select *Local* from the drop-down list box and then click ***Local User Setting*** button to enter the **Local User Settings**. Then, click the hyperlink of ***Edit Local User List.***

Enabling two or more servers of the same authentication method is NOT allowed.

© 2008 4IPNET, INC.

4.2.1.1 Authentication Method – Local

Choose **"Local User"** from the **Authentication Method** field, the button besides the drop-down menu will become **"Local User Setting"**.

Authentication Option - Server 1		
Name	Server 1 *	
Postfix	local *	
Black List	None	
Authentication Database	Local	Configure
Group	Group 1	

Click the button of ***Local User Setting*** for further configuration.

Local User Database Settings	
Local User List	
Account Roaming Out	Enable Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	Enable Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

- **Edit Local User List:** It will let the administrator view / add, and delete local user account. The ***Upload User*** button is for importing a list of user accounts from a text file. The ***Download User*** button is for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account. Local user account can be assigned a policy and applied Local VPN individually. Check the check box of individual local user account in the Enable Local VPN column to enable individually. MAC address of a networking device can be bound with a local user as well.

© 2008 4IPNET, INC.

Add User | Upload User | Download User

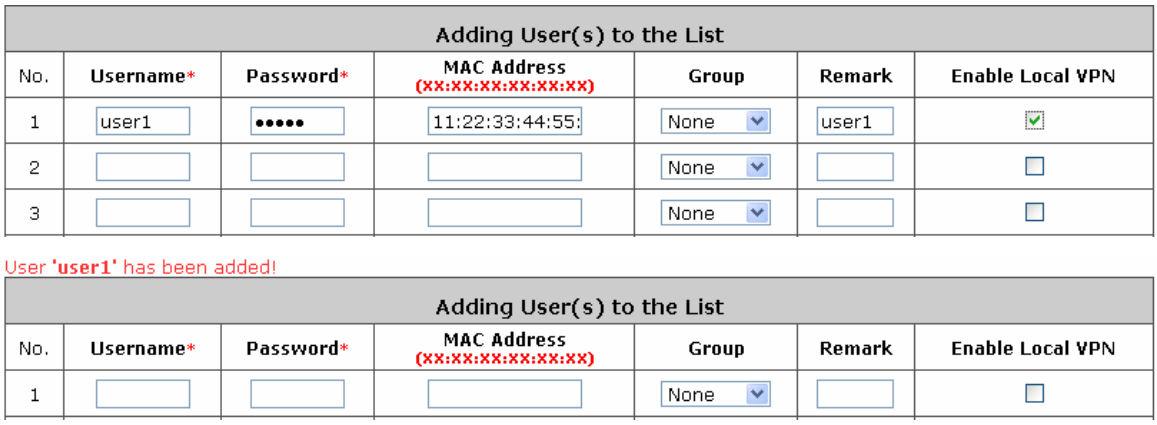
Search

Local User List				
Username	Password	MAC Address	Applied Group Local VPN Enabled Remark	Del All
user1	user1	11:22:33:44:55:66	None Yes user1	Delete
user2	user2		Group 1 No user2	Delete
test	1234	00:00:00:00:00:00	None No	Delete

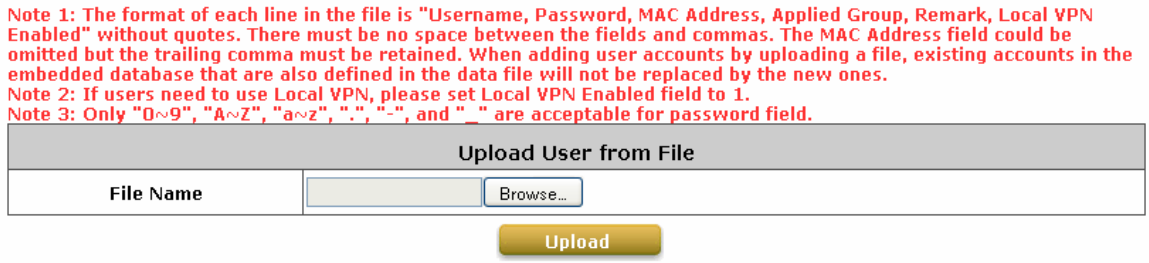
© 2008 4IPNET, INC.

- ***Add User*:** Click this button to enter into the **Adding User(s) to the List** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"**, and **"Remark"**. Select a desired **Group** to classify local users. Check to enable *Local VPN* in the **Enable Local VPN** column. Click ***Apply*** to complete adding the user(s).

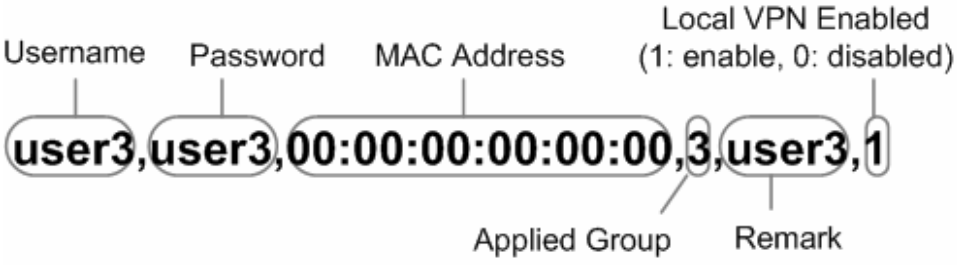
  For more information on Group configuration, please refer to **4.2.3. Group Configuration**.



- **Upload User:** Click ***Upload User*** to enter the **Upload User from File** interface. Click the ***Browse*** button to select the text file for uploading user accounts, then click ***Upload*** to complete the upload process.

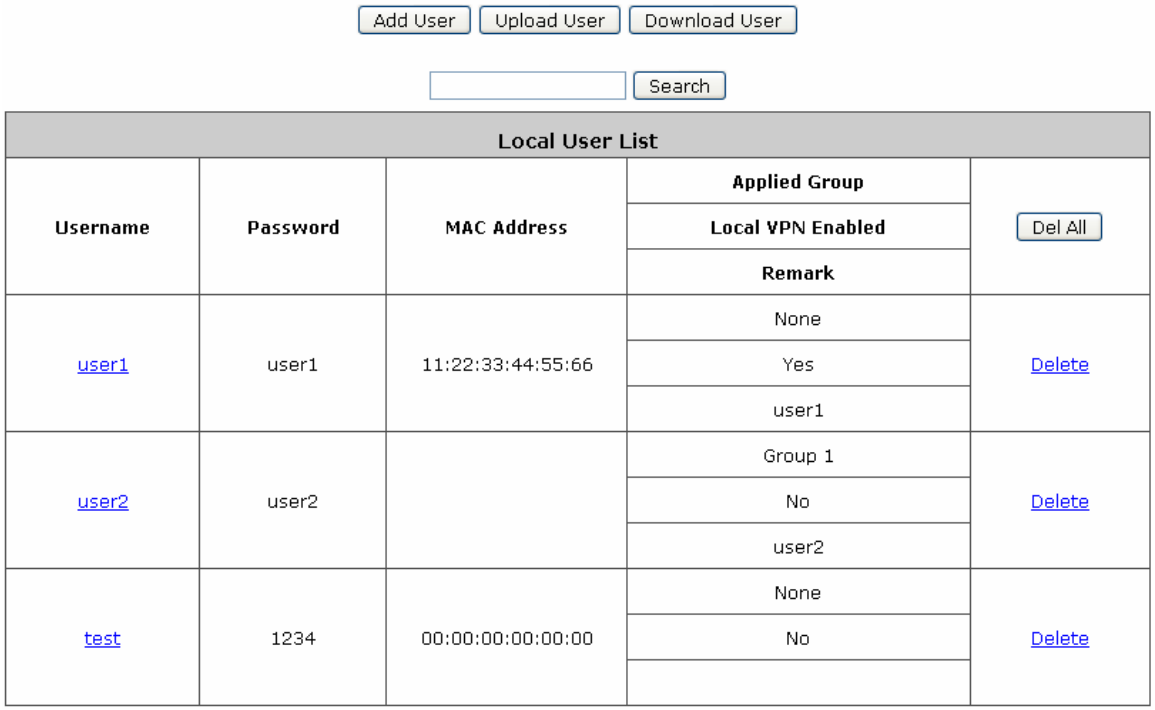

Note 1: The format of each line in the file is "Username, Password, MAC Address, Applied Group, Remark, Local VPN Enabled" without quotes. There must be no space between the fields and commas. The MAC Address field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.
Note 2: If users need to use Local VPN, please set Local VPN Enabled field to 1.
Note 3: Only "0~9", "A~Z", "a~z", ".", "-", and "_" are acceptable for password field.
Upload User from File
File Name
Browse...
Upload

When uploading a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, and then, try again. The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

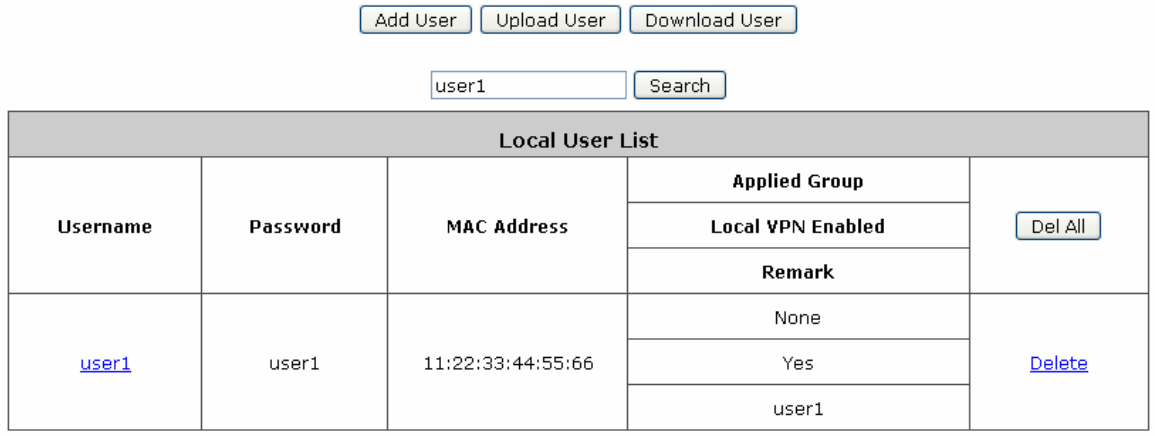


© 2008 4IPNET, INC.

- ***Download User***: Use this function to create a .txt file with all built-in user account information and then save it on disk.



- ***Search***: Enter a keyword of a username to be searched in the text field and click this button to perform the search. All usernames matching the keyword will be listed.



- ***Del All***: Click on this button to delete all the users at once and click on ***Delete*** to delete the user individually.

© 2008 4IPNET, INC.

- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account to enter the **User Profile** Interface for that particular user, and then modify or add any desired information such as *Username*, *Password*, *MAC Address* (optional), *Group* (optional), *Enable Local VPN* (optional) and *Remark* (optional). Click ***Apply*** to complete the modification.

Editing Existing User Data	
Username	user1 *
Password	user1 *
MAC Address	11:22:33:44:55:66
Applied Group	None
Enable Local VPN	☑
Remark	user1

- **Roaming Out & 802.1X Authentication:** When Account Roaming Out is enabled, the link of this function will be available to define the authorized device with IP address, Subnet Mask, and Secret Key. Please see more explanation above in the section for **Roaming Out** and the section for **802.1X Authentication**.

Local User Database Settings	
Local User List	
Account Roaming Out	◉ Enable ○ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	○ Enable ◉ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
Roaming Out & 802.1X Client Device Settings	

Roaming Out & 802.1x Client Device Settings				
No.	Type	IP Address	Subnet Mask	Secret Key
1	Roaming Out		255.255.255.255 (/32)	••••
2	802.1X	192.168.0.0	255.255.255.254 (/31)	••••

Click the hyperlink ***RADIUS Client List*** to enter the **Radius Client Configuration** interface. Choose the desired type, **Disable**, **Roaming Out** or **802.1X**, and key in the 802.1X client's IP address and network mask and then click ***Apply*** to complete the settings.

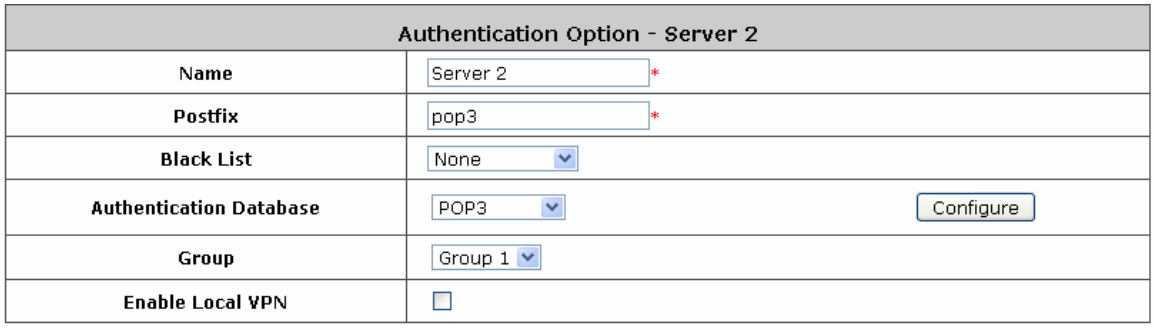
802.1X Authentication: When **802.1X Authentication** is enabled, the Local authentication database will be used as a RADIUS database for connection with 802.1X enabled devices such as APs or switches.

Roaming Out: The system's local user database can also be an external RADIUS database to another system. When *Account Roaming Out* is enabled, local users can login from other domains with their original local user accounts. The authentication database with their original local user accounts acts as a RADIUS Server and roaming out local users act as RADIUS clients.

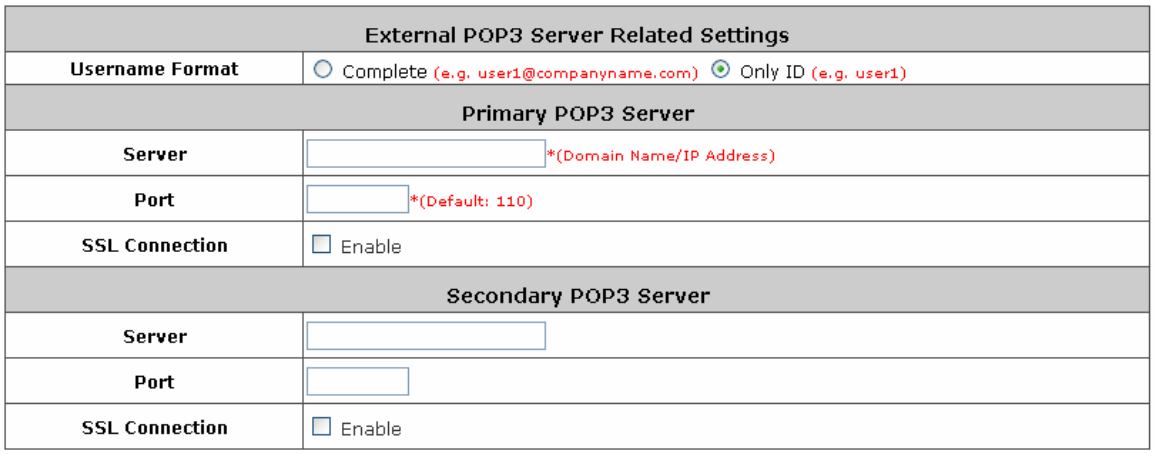
© 2008 4IPNET, INC.

4.2.1.2 Authentication Method – POP3

Choose **"POP3"** from the **Authentication Method** field, the button beside the drop-down menu will become **"POP3 Setting"**.



Click the button of ***POP3 Setting*** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



- **Server IP:** The IP address of the external POP3 Server.
- **Port:** The authentication port of the external POP3 Server.
- **SSL Setting**: The system supports POP3S. Check the check box beside to **Enable SSL Connection** to POP3.

© 2008 4IPNET, INC.

4.2.1.3 Authentication Method – RADIUS

Choose **"RADIUS"** from the **Authentication Method** field, the button beside the drop-down menu will become **"Radius Setting"**.

Authentication Option - Server 3	
Name	Server 3 *
Postfix	radius *
Black List	None
Authentication Database	RADIUS Configure
Group	Group 1
Enable Local VPN	☐

Click the button of ***Radius Setting*** for further configuration. The RADIUS server sets the external authentication for user accounts. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.

External RADIUS Server Related Settings	
802.1X Authentication	Enable Disable
Username Format	Complete (e.g. user1@companyname.com) Only ID (e.g. user1)
NAS Identifier	
NAS Port Type	19 *(Default 19, Range: 0~35)
Class-Group Mapping	Edit Class-Group Mapping
Primary RADIUS Server	
Server	*(Domain Name/IP Address)
Authentication Port	*(Default: 1812)
Accounting Port	*(Default: 1813)
Secret Key	*
Accounting Service	Enable Disable
Authentication Protocol	PAP
Secondary RADIUS Server	
Server	(Domain Name/IP Address)
Authentication Port	
Accounting Port	
Secret Key	
Accounting Service	Enable Disable
Authentication Protocol	CHAP

802.1X Authentication: The system supports 802.1X. When *802.1X Authentication* is enabled, the Local Authentication Database will be used as a RADIUS database for connection with 802.1X enabled devices such as access points or switches.

When the option is enabled, the hyperlink of ***Radius Client List*** will appear.

Click the hyperlink of ***Radius Client List*** to enter the ***Radius Client Configuration*** page. Choose a desired type

© 2008 4IPNET, INC.

from *Disable*, *Roaming Out* or *802.1X*. Enter the *IP Address*, Segment (*Subnet Mask),* and *Secret Key* of 802.1X clients. Click ***Apply*** to complete the settings.

Roaming Out & 802.1x Client Device Settings				
No.	Type	IP Address	Subnet Mask	Secret Key
1	Roaming Out		255.255.255.255 (/32)	••••
2	802.1X	192.168.0.0	255.255.255.254 (/31)	••••

- **Trans Full Name:** When ***Complete*** option is checked, both the username and postfix will be transferred to the RADIUS server for authentication. On the other hand, when ***Only ID*** option is checked, only the username will be transferred to the external RADIUS server for authentication.
- **NASID:** The Network Access Server (NAS) Identifier of the system for the external RADIUS server.
- **NAS Port Type:** The type of physical port used by NAS to authenticate the user..
- **Class-Group Mapping**
- This function is to assign a *Group* to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to its assigned Group.

RADIUS Group Mapping - Server 3			
◉ Enable ○ Disable			
No.	Class Attribute Value	Group	Remark
1	GROUP_1	Group 1	MANAGEMENT
2	GROUP_2	Group 2	EMPLOYEES
3	GROUP_3	Group 3	GUEST
4		Group 1	
5		Group 1	
6		Group 1	
7		Group 1	
8		Group 1	

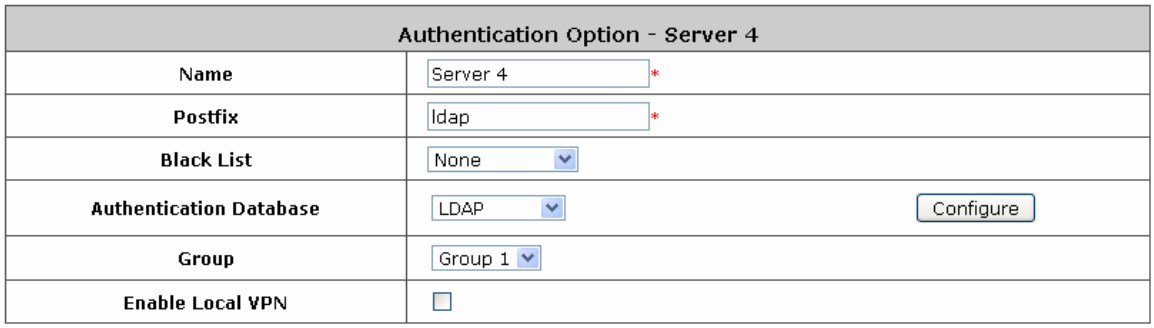
- **Server IP:** The IP address of the external RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server.
- **Accounting Port:** The accounting port of the external RADIUS server.
- **Secret Key:** The Secret Key for RADIUS authentication.
- **Accounting Service:** The system supports RADIUS accounting that can be enabled or disabled.
- **Authentication Protocol:** The configuration of the system must match with that of the remote RADIUS server. **PAP** (Password Authentication Protocol) transmits passwords in plain text without encryption. **CHAP** (Challenge Handshake Authentication Protocol) is a more secure authentication protocol with hash encryption.

Note: If the RADIUS Server does not assign idle-timeout value, the WHG303 will use the local idle-timeout.

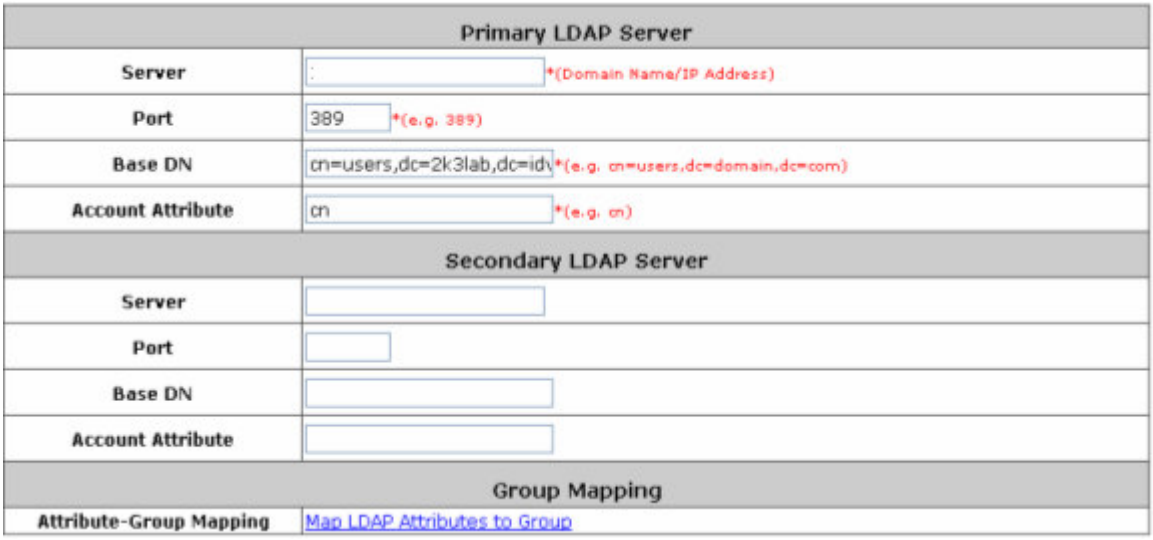
© 2008 4IPNET, INC.

4.2.1.4 Authentication Method – LDAP

Choose **"LDAP"** from the **Authentication Method** field, the button beside the drop-down menu will become **"LDAP Setting"**.



Click the button of ***LDAP Setting*** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisk are necessary information which should be filled in. These settings will become effective immediately after clicking the ***Apply*** button.



- **Server IP:** The IP address of the external LDAP server.
- **Port:** The authentication port of the external LDAP server.
- **Base DN:** The Distinguished Name for the navigation path of LDAP account.
- **Account Attribute**: The attribute of LDAP accounts.
- **Attribute-Group Mapping**: This function is to assign a *Group* to a LDAP attribute sent from the LDAP server. When the clients classified by LDAP attributes log into the system via the LDAP server, each client will be mapped to its assigned Group. To get and show the attribute name and value from the configured LDAP server, enter *Username* and *Password* and click ***Show Attribute***. Then, the table of attribute will be displayed. Enter the *Attribute Name* and *Attribute Value* chosen from the attribute table, and select a *Group* from the drop-down list box.

© 2008 4IPNET, INC.

Attribute Name	Attriubute Value
CN	USER01
C	TW

LDAP Group Mapping - Server 4

○ Enable ◉ Disable

No.	LDAP Attribute Name	LDAP Attribute Value	Group	Remark
1	CN	USER01	Group 1	
2	C	TW	Group 2	

© 2008 4IPNET, INC.

4.2.1.5 Authentication Method – NTDomain

Choose **"NTDomain"** from the **Authentication Method** field, the button beside the drop-down menu will become **"NT Domain Setting"**.

Authentication Option - Server 4	
Name	Server 4 *
Postfix	ldap *
Black List	None
Authentication Database	NT Domain Configure
Group	Group 1
Enable Local VPN	☐

Click the button of ***NT Domain Setting*** for further configuration. Enter the server IP address and enable/disable the transparent login function. These settings will become effective immediately after clicking the ***Apply*** button.

Domain Controller	
Server	*(IP Address)
Transparent Login	Enable Disable (Windows 2000, 2003 or above)

- **Server IP:** The IP address of the external NT Domain Server.
- **Transparent Login:** This function refers to Windows NT Domain single sign on. When *Transparent Login* is enabled, clients will log in to the system automatically after they have logged in to the NT domain, which means that clients only need to log in once.

© 2008 4IPNET, INC.

4.2.1.6 Authentication Method – On-demand User

On-demand User Server Configuration: The administrator can enable and configure this authentication method to create on-demand user accounts. This function is designed for hotspot owners to provide temporary users with free or paid wireless Internet access in the hotspot environment. Major functions include accounts creation, users monitoring list, billing plan, billing report statistics, and external payment gateway support.

Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account List	View

1) **General Settings**

This is the common setting for the On-demand User authentication option. The generated on-demand users and all accounts related information such as postfix and unit will be shown in this list.

General Settings	
Postfix	ondemand
Monetary Unit	None $ USD £ GBP € EUR (Input other desired monetary unit, e.g. AU)
Group Name	Group 1
WLAN ESSID	4ipnet
Wireless Key	
Remaining Volume Sync Interval	10min(s) 15min(s) 20min(s)
Terminal Server	Configuration

- **Postfix:** Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Enter the postfix used for on-demand users.
- **Monetary Unit:** Select the desired monetary unit or specified the unit by users.
- **Group Name:** Select the desired group for on-demand user.
- **WLAN ESSID:** The administrator can enter the defined wireless ESSID in this field and it will be printed on the receipt for on-demand users' reference when accessing the Internet via wireless LAN service. The ESSIDs given here should be those of the Service Zones enabled for On-demand Users.
- **Wireless Key:** The administrator can enter the defined wireless key such as WEP or WPA in the field. The Wireless Key will be printed on the receipt for the on-demand users' reference when accessing the Internet via wireless LAN service.
- **Remaining Volume Sync Internal:** While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.
- **Number of Tickets:** Print one or duplicate receipts, when pressing the print button of the ticket printer

© 2008 4IPNET, INC.

which connected to serial port.

- **Terminal Server:** The ticket terminal can be enhanced with serial ticket printing over Ethernet. Terminal Server is a list of serial-to-Ethernet devices that communicate with the system only; never get online and no need to go through authentication.
  For customers making purchase at the front desk in a hotel, a receptionist uses an account generator (192.168.2.1) to create a guest account and print out receipts with account information. A client in the other floor can print the same receipt without going to the front desk on the lobby by using the second floor account generator (192.168.2.2). Both account generators work for the system on LAN side.

Terminal Server Configuration				
Item	Server IP	Port	Location	Remark
1	192.168.2.1	100	1st_fl_info_desk	Tom ext 359
2	192.168.2.2	100	2nd_fl	Jerry
3				

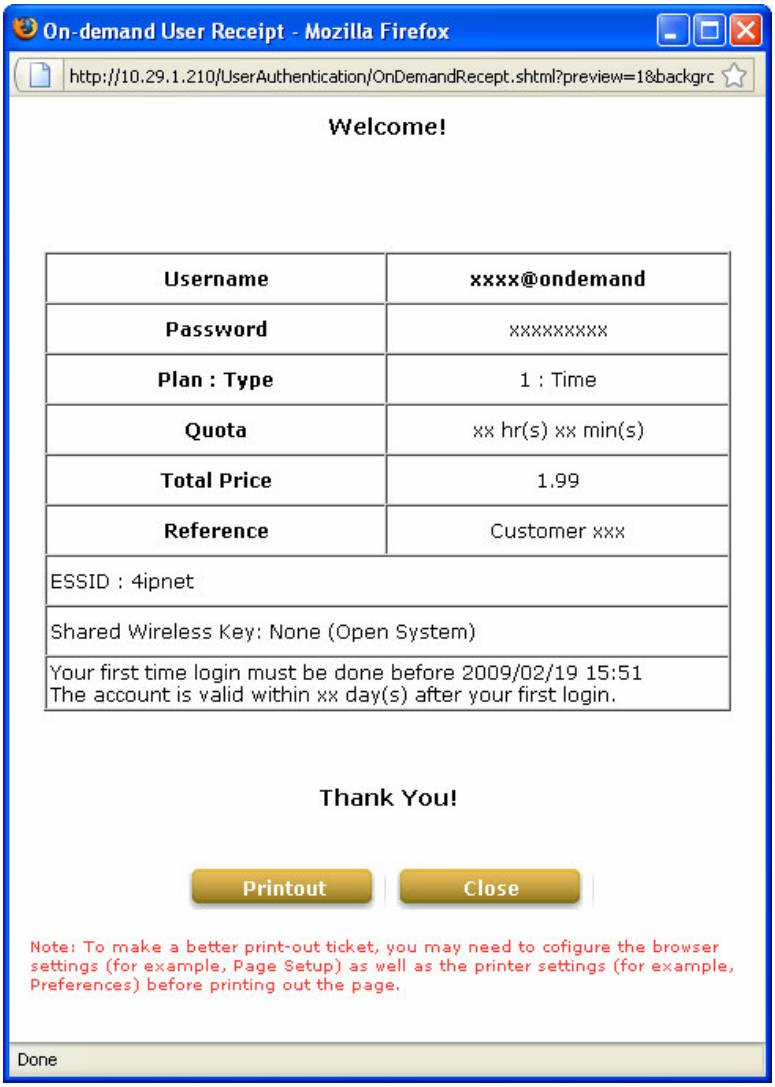
2) **Ticket Customization**

On-demand account ticket can be customized here and previewed on the screen.

Ticket Customization	
Receipt Header 1	Welcome!
Receipt Header 2	
Receipt Header 3	
Receipt Footer 1	Thank You!
Receipt Footer 2	
Receipt Footer 3	
Remark	
Background Image	○ None ◉ Default Image ○ Uploaded Image [Edit]
Twin Ticket	○ Enable ◉ Disable

[Preview]

© 2008 4IPNET, INC.


On-demand User Receipt - Mozilla Firefox
http://10.29.1.210/UserAuthentication/OnDemandRecept.shtml?preview=1&backgrc
Welcome!
Username
xxxx@ondemand
Password
xxxxxxxxx
Plan : Type
1 : Time
Quota
xx hr(s) xx min(s)
Total Price
1.99
Reference
Customer xxx
ESSID : 4ipnet
Shared Wireless Key: None (Open System)
Your first time login must be done before 2009/02/19 15:51
The account is valid within xx day(s) after your first login.
Thank You!
Printout
Close
Note: To make a better print-out ticket, you may need to cofigure the browser settings (for example, Page Setup) as well as the printer settings (for example, Preferences) before printing out the page.
Done

- **Receipt Header:** There are two receipt headers supported by the system. The entered content will be printed on the receipt. These headers are optional.
- **Receipt Footer:** The entered content will be printed on the receipt. This footer is optional.
- **Background Image:** You can choose to customize the ticket by uploading your own background image for the ticket, or choose the default image or none. Click Browse to select the image file and then click upload. The background image file size limit is 100 Kbytes. No limit for the dimensions of the image is set, but a 460x480 image is recommended.
- **Twin Ticket**: Enable this function to print duplicate receipts.
- **Preview:** Click ***Preview*** button, the ticket will be shown including the information of username and password with the selected background. Print the ticket here.

© 2008 4IPNET, INC.

3) Billing Plans

Administrators can configure several billing plans. Click ***Edit*** button to enter the page of Editing Billing Plan. Click ***Apply*** to save the plan that manually set up by the administrators. Go back to the screen of Billing Plans, click ***Enable*** button, and then the plan is activated.

Billing Plans

Plan	Type	Quota	Price	Enable	Function
1	Time	2 hrs 0 mins	20	☑	Edit
2	N/A			☐	Edit
3	N/A			☐	Edit
4	N/A			☐	Edit
5	N/A			☐	Edit
6	N/A			☐	Edit
7	N/A			☐	Edit
8	N/A			☐	Edit
9	N/A			☐	Edit
0	N/A			☐	Edit

- **Plan:** The number of the specific plan.
- **Type:** This is the type of the plan, based on which it defines how the account can be used.
- **Quota:** The limit on how On-demand users are allowed to access the network.
- **Enable:** Click the radio button to activate the plan.
- **Function:** Click the button ***Edit*** to add one billing plan.
  - **Time:** Total period of time (xx hrs yy mins), during which On-demand users are allowed to access the network.

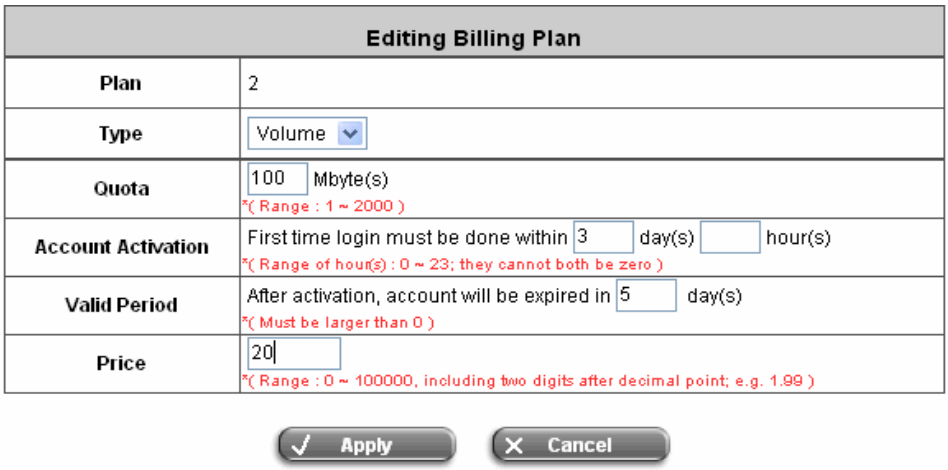
Editing Billing Plan

Plan	1
Type	Time
Quota	2 hr(s) 0 min(s) *(Range of min(s) : 0 ~ 59; they cannot both be zero)
Account Activation	First time login must be done within 3 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 5 day(s) *(Must be larger than 0)
Price	20 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

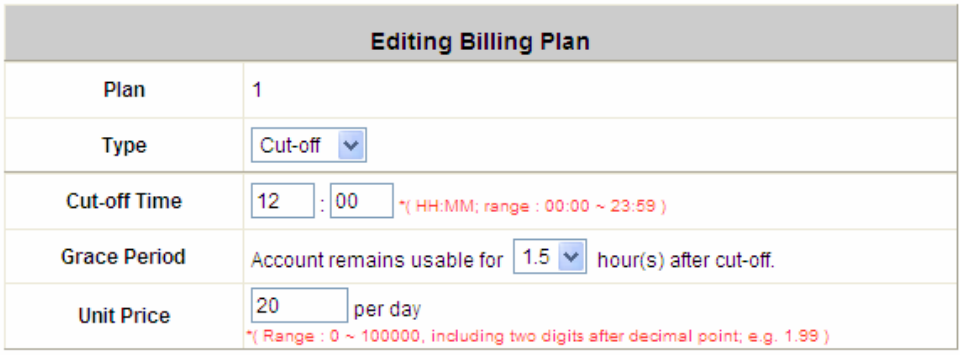
Apply Cancel

  - **Volume:** Total traffic volume (xx Mbytes), up to which on-demand users are allowed to transfer data.

© 2008 4IPNET, INC.


Editing Billing Plan
Plan
2
Type
Volume
Quota
100 Mbyte(s)
*(Range : 1 ~ 2000)
Account Activation
First time login must be done within 3 day(s) hour(s)
*(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period
After activation, account will be expired in 5 day(s)
*(Must be larger than 0)
Price
20
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Apply
Cancel

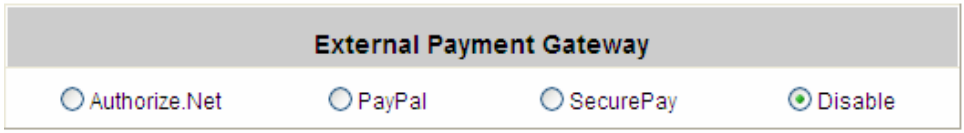
- **Cut-off Time:** The time of day at which the on-demand account is cut off (made expired) by the system on that day. Please note that the "Grace Period" is an additional, short period of time after the account is cut off, during which a user is allowed to continue to use the on-demand account to access the Internet without paying additional fee.


Editing Billing Plan
Plan
1
Type
Cut-off
Cut-off Time
12 : 00 *(HH:MM; range : 00:00 ~ 23:59)
Grace Period
Account remains usable for 1.5 hour(s) after cut-off.
Unit Price
20 per day
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

4) External Payment Gateway

This section is for merchants to set up an external payment gateway to accept payments in order to provide wireless access service to end customers who wish to pay for the service on-line.

Three payment selections include **Authorize.Net**, **PayPal, Secure Pay** and **Disable**. The default is ***Disable***.

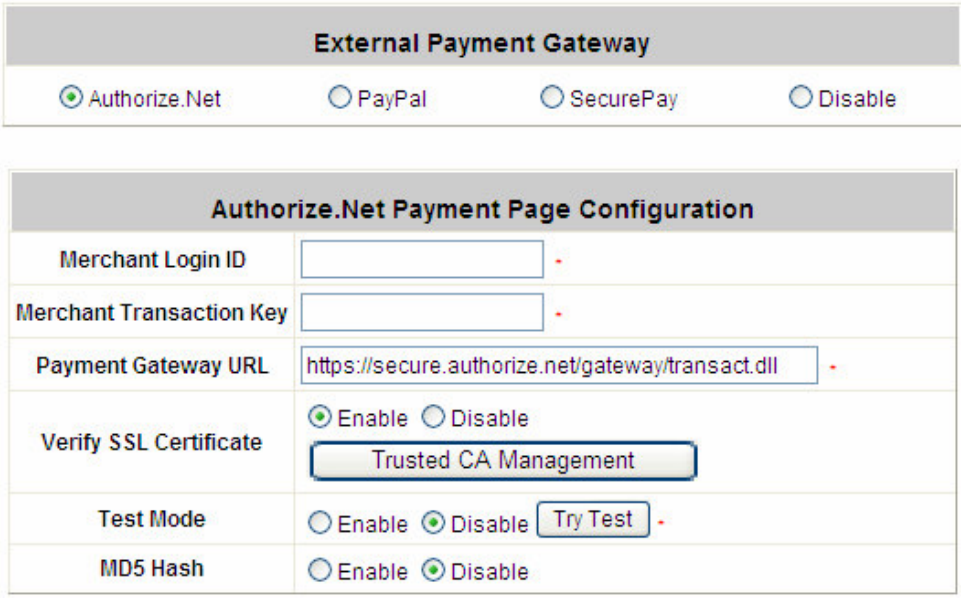


- **Authorize.Net**

Before setting up "Authorize.Net", it is required that the merchant owners have a valid Authorize.Net account. Please see ***Appendix A. Accepting Payments via Authorize.Net*** for more information about opening an Authorize.Net account, relevant maintenance functions, and an example for end users.

© 2008 4IPNET, INC.

➢ **Authorize.Net Payment Page Configuration**



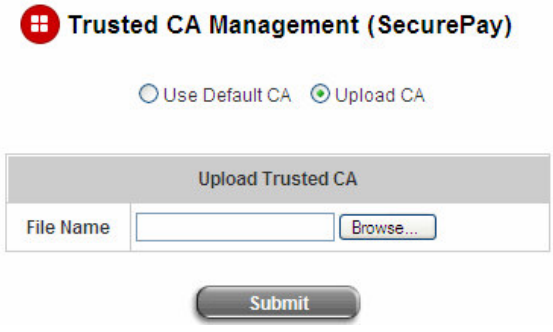
Merchant ID: This is the "Login ID" that comes with the Authorize.Net account

Merchant Transaction Key: The merchant transaction key is similar to a password and is used by Authorize.Net to authenticate transactions.

Payment Gateway URL: This is the default website address to post all transaction data.

Verify SSL Certificate: This is to help protect the system from accessing a website other than Authorize.Net.

- **Trusted CA Management:** Select the version of Trusted Certificate for the system.

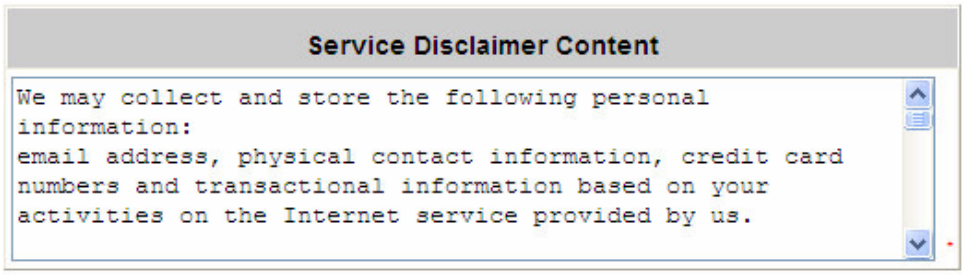


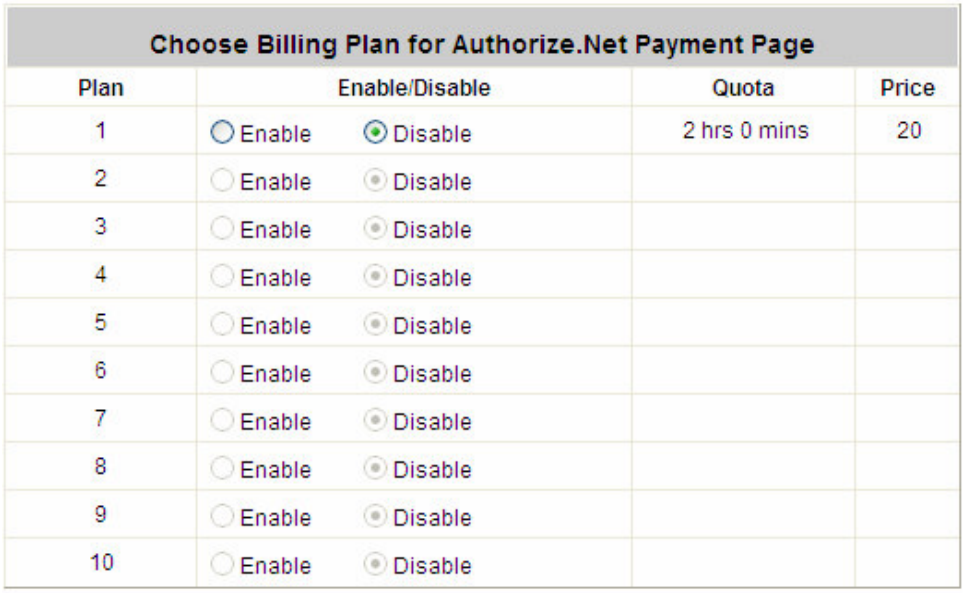
Test Mode: In this mode, merchants can post **test** transactions **for free** to check if the payment function works properly.

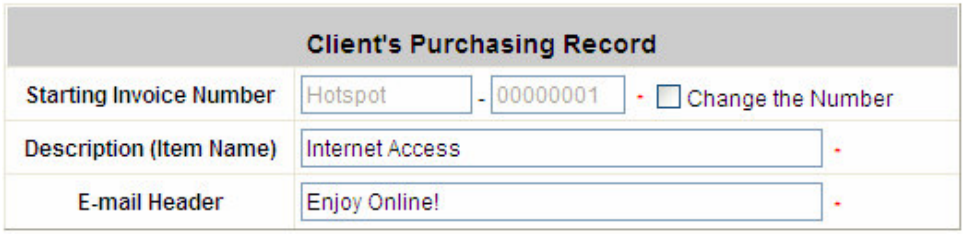
MD5 Hash: If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction, or transaction response, received by their server were actually sent from the Authorize.Net.

© 2008 4IPNET, INC.

- **Service Disclaimer Content/ Choose Billing Plan for Authorize.Net Payment Page/Client's Purchasing Record**


Service Disclaimer Content
We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.





Service Disclaimer Content

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

Choose Billing Plan for Authorize.Net Payment Page

These 10 plans are the plans configured in **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.

Client's Purchasing Record

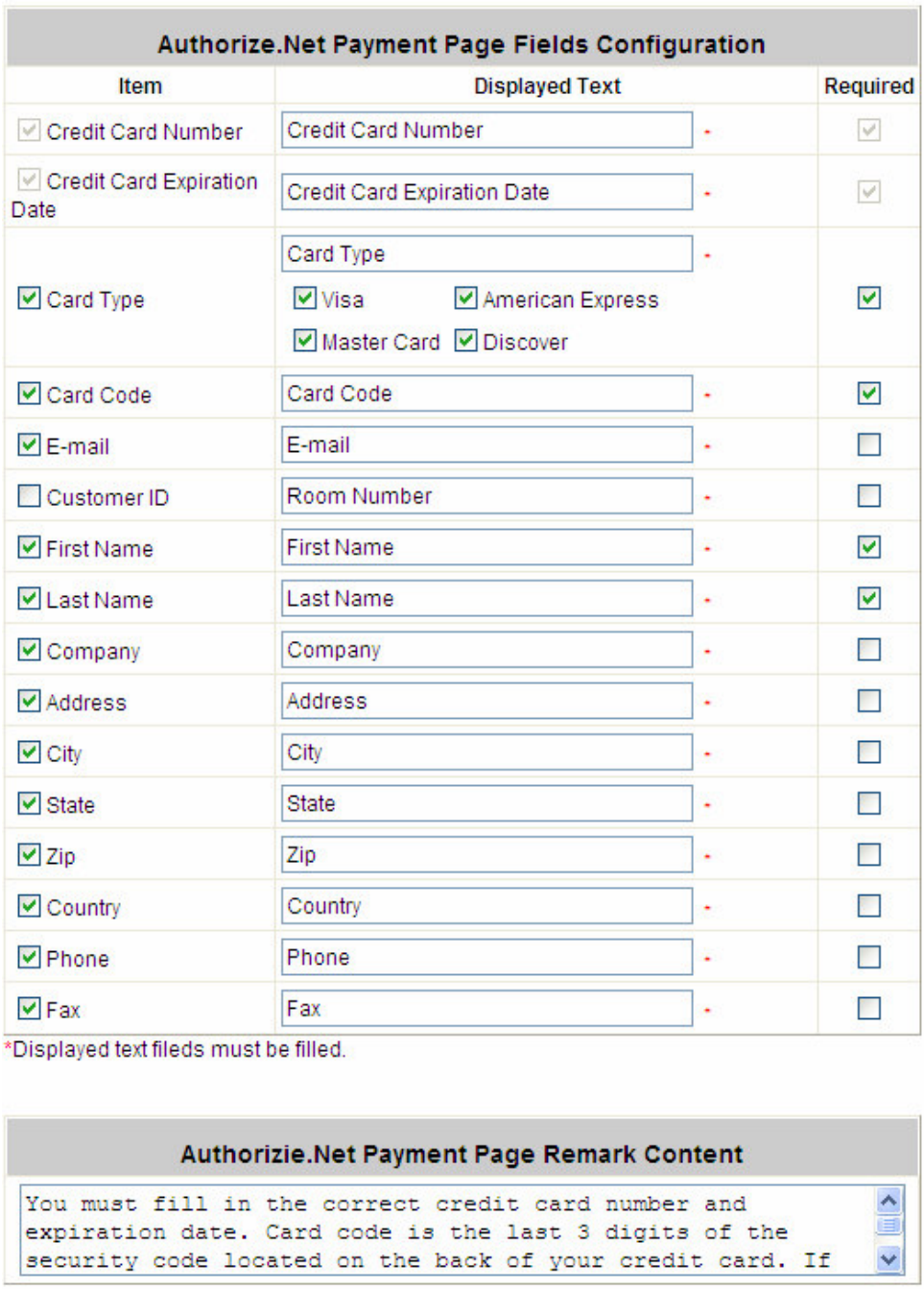
Starting Invoice Number: An invoice number may be provided as additional information with a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.

Description (Item Name): This is the item information to describe the product (for example, Internet Access).

© 2008 4IPNET, INC.

Email Header: Enter the information that should appear in the header of the invoice.

- **Authorize.Net Payment Page Fields Configuration/ Authorize.Net Payment Page Remark Content**



Authorize.Net Payment Page Fields Configuration

Item	Displayed Text	Required
Credit Card Number	Credit Card Number -	
Credit Card Expiration Date	Credit Card Expiration Date -	
Card Type	Card Type - Visa, American Express, Master Card, Discover	
Card Code	Card Code -	
E-mail	E-mail -	
Customer ID	Room Number -	
First Name	First Name -	
Last Name	Last Name -	
Company	Company -	
Address	Address -	
City	City -	
State	State -	
Zip	Zip -	
Country	Country -	
Phone	Phone -	
Fax	Fax -	

*Displayed text fileds must be filled.

Authorizie.Net Payment Page Remark Content

You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If

- **Authorize.Net Payment Page Fields Configuration**

Item: Check the box to show this item on the customer's payment interface.

Displayed Text: Enter what needs to be shown for this field.

Required: Check the box to indicate this item as a required field.

Credit Card Number: Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

Credit Card Expiration Date: Month and year expiration date of the credit card. This should be entered in

© 2008 4IPNET, INC.

the format of MMYY. For example, an expiration date of July September 2009 should be entered as 0709.

Card Type: This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.

Card Code: The three- or four-digit code assigned to a customer's credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

E-mail: An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.

Customer ID: This is an internal identifier for a customer that may be associated with the billing information of a transaction. This field may contain any format of information.

First Name: The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

Last Name: The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

Company: The name of the company associated with the billing or shipping information entered on a given transaction.

Address: The address entered either in the billing or shipping information of a given transaction.

City: The city is associated with either the billing address or shipping address of a transaction.

State: A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

Zip: The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

Country: The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

Phone: A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

Fax: A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

- **Authorizie.Net Payment Page Remark Content**

  Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

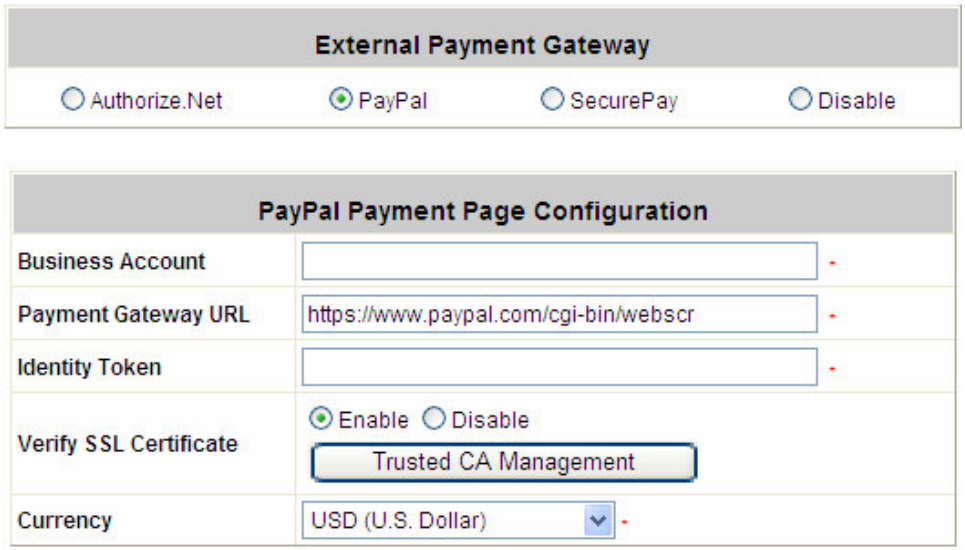
© 2008 4IPNET, INC.

- **PayPal**

  Before setting up "PayPal", it is required that the hotspot owners have a valid PayPal "Business Account". Please see ***Appendix B. Accepting Payments via PayPal*** for more information about setting up a PayPal Business Account, relevant maintenance functions, and an example for clients.

  After opening a PayPal Business Account, the hotspot owners should find the **"Identity Token"** of this PayPal account to continue "PayPal Payment Page Configuration".

  - **External Payment Gateway / PayPal Payment Page Configuration**



Business Account: The "Login ID" (an email address) that is associated with the PayPal Business Account.

Payment Gateway URL: The default website address to post all transaction data.

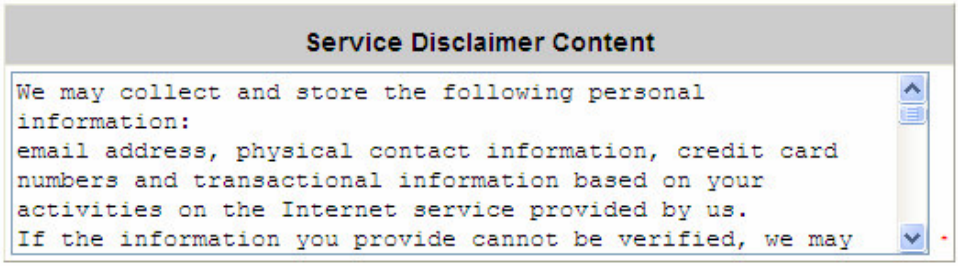
Identity Token: This is the key used by PayPal to validate all the transactions.

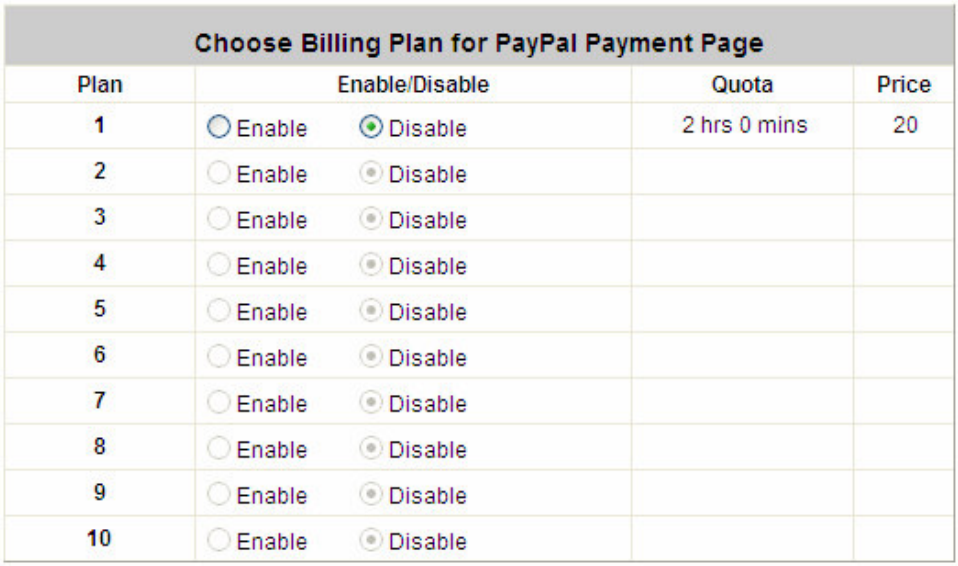
Verify SSL Certificate: This is to help protect the system from accessing a website other than PayPal

Currency: The currency to be used for the payment transactions.

© 2008 4IPNET, INC.

- **Service Disclaimer Content / Billing Configuration for Payment Page**

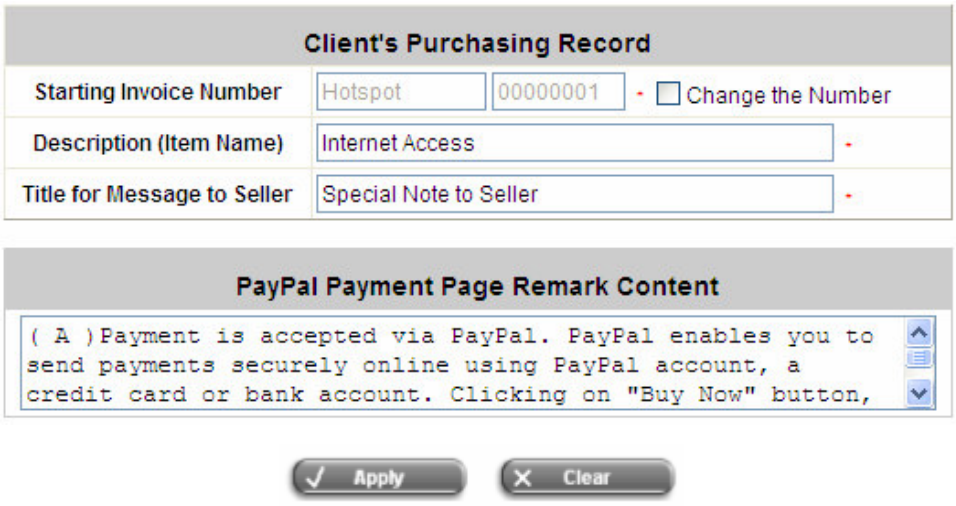

Service Disclaimer Content
We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may



Service Disclaimer Content: View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

Choose Billing Plan for PayPal Payment Page: These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

- **Client's Purchasing Record / PayPal Payment Page Remark Content**


Client's Purchasing Record
Starting Invoice Number
Hotspot
00000001
Change the Number
Description (Item Name)
Internet Access
Title for Message to Seller
Special Note to Seller
PayPal Payment Page Remark Content
(A)Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button,
Apply
Clear

Client's Purchasing Record:

Invoice Number: An invoice number may be provided as additional information against a transaction.

© 2008 4IPNET, INC.

This is a reference field that may contain any kind of information.

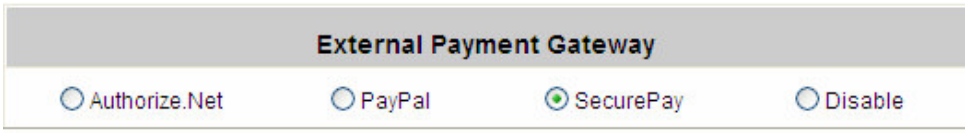
Description: Enter the product/service description (e.g. wireless access service).

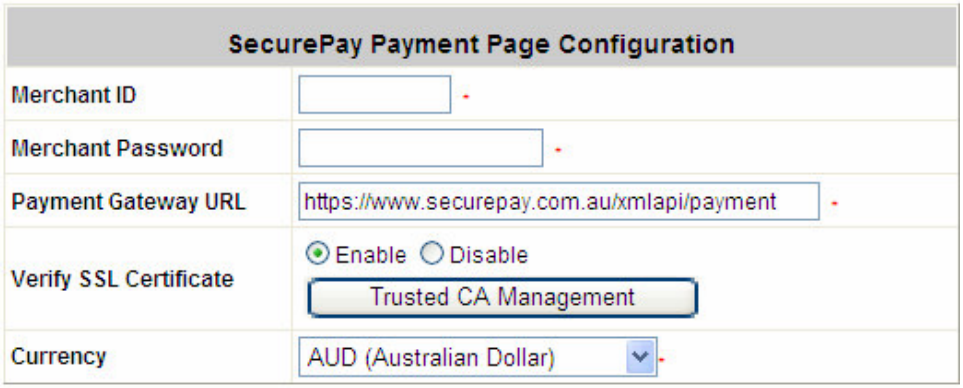
Title for Message to Seller: Enter the information that will appear in the header of the PayPal payment page.

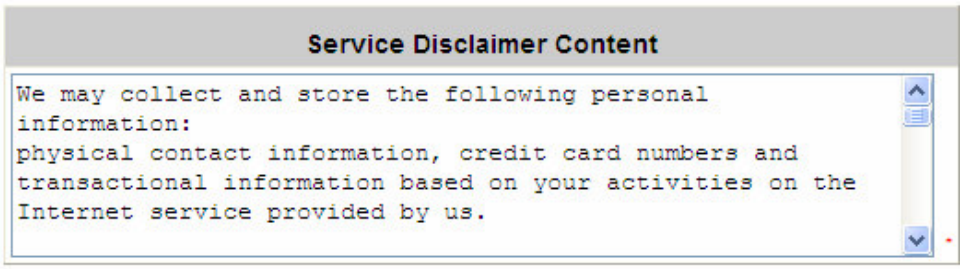
PayPal Payment Page Remark Content: The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe the cautions for making a payment via PayPal.

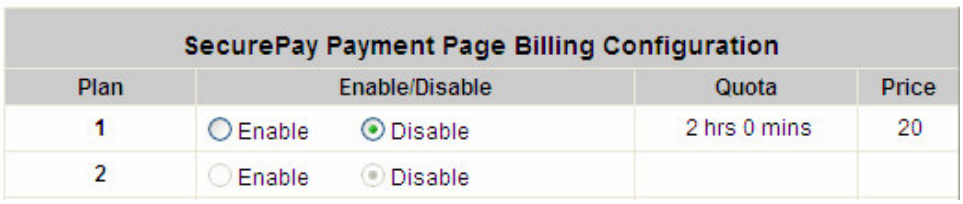
- **SecurePay**

Before setting up "SecurePay", it is required that the hotspot owners have a valid SecurePay "Merchant Account" from its official website. Please see ***Appendix C. Accepting Payments via SecurePay*** for more information about setting up a SecurePay Account, relevant maintenance functions, and an example for clients.

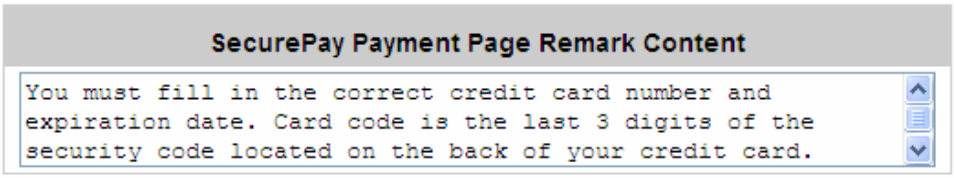





Service Disclaimer Content
We may collect and store the following personal information:
physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.



© 2008 4IPNET, INC.


SecurePay Payment Page Remark Content
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.

- **Payment Page Configuration**

  Merchant ID: The ID that is associated with the Business Account.

  Password: This is the key used by SecurePay to validate all the transactions.

  Payment Gateway URL: The default website address to post all transaction data.

  Verify SSL Certificate: This is to help protect the system from accessing a website other than SecurePay.

  Currency: The currency to be used for the payment transactions.

- **Service Disclaimer Content**

  View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

- **SecurePay Payment Page Billing Configuration**

  These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

- **SecurePay Payment Page Remark Content**

  The message content will be displayed as a special notice to end customers.

5) **On-demand Account Creation**

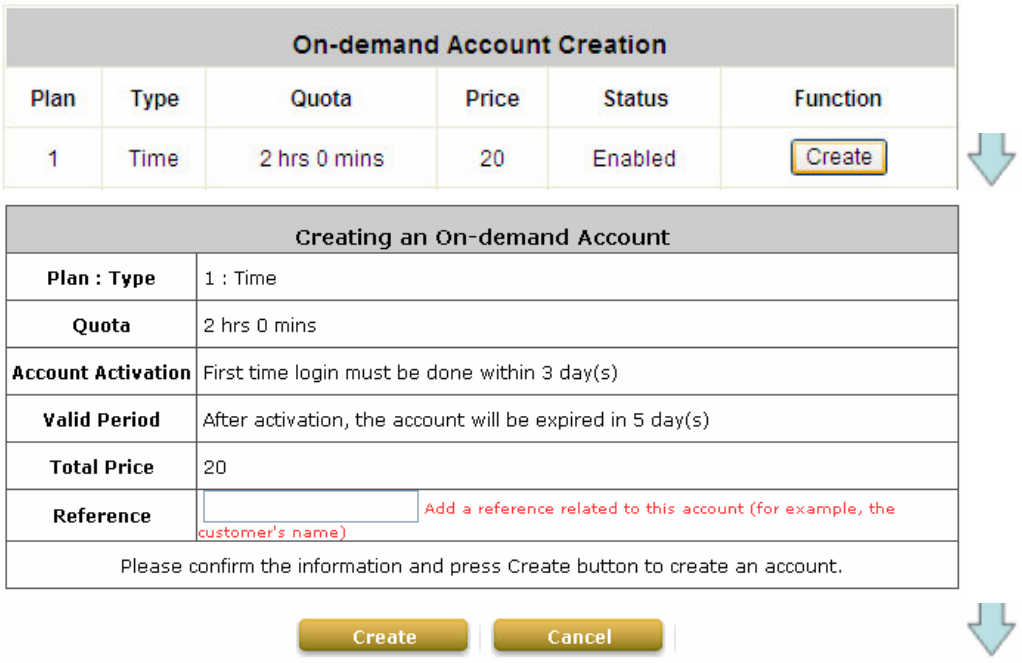
On-demand accounts are listed and related. When at least one plan is enabled, the administrator can generate on-demand user accounts here. Click this to enter the On-demand Account Creation screen. Click on the ***Create*** button of the desired plan and an on-demand user account will be created. Click ***Print*** to print a receipt which will contain the on-demand user's information, including the username and password.

Note: If no Billing plan is enabled, accounts cannot be created by clicking ***Create*** button. Please goes back to Billing Plans to active at least one Billing plan by clicking ***Edit*** button and ***Apply*** the setting to activate the plan. The printer used by ***Print*** is a pre-configured printer connected to the administrator's computer.

© 2008 4IPNET, INC.

On-demand Account Creation					
Plan	Type	Quota	Price ($)	Status	Function
1	Time	1 hr(s) 2 min(s)	2	Enabled	Create
2	Time	12 hr(s)	3.99	Enabled	Create
3	Volume	500 Mbyte(s)	5	Enabled	Create
4	N/A	N/A	N/A	Disabled	Create
5	N/A	N/A	N/A	Disabled	Create
6	N/A	N/A	N/A	Disabled	Create
7	N/A	N/A	N/A	Disabled	Create
8	N/A	N/A	N/A	Disabled	Create
9	N/A	N/A	N/A	Disabled	Create
0	N/A	N/A	N/A	Disabled	Create

- **Plan:** The number of a specific plan.
- **Type:** Show one type of the plan in Time, Volume or Cut-off.
- **Quota:** The Time Volume is how long the on-demand user is allowed to access the Internet.
- **Price:** The unit price of each plan.
- **Status:** Show the status in enabled or disabled.
- **Function:** Press ***Create*** button for the desired plan; an On-demand user account will be created, and then click ***Printout*** to print a receipt which will contain this on-demand user's information.

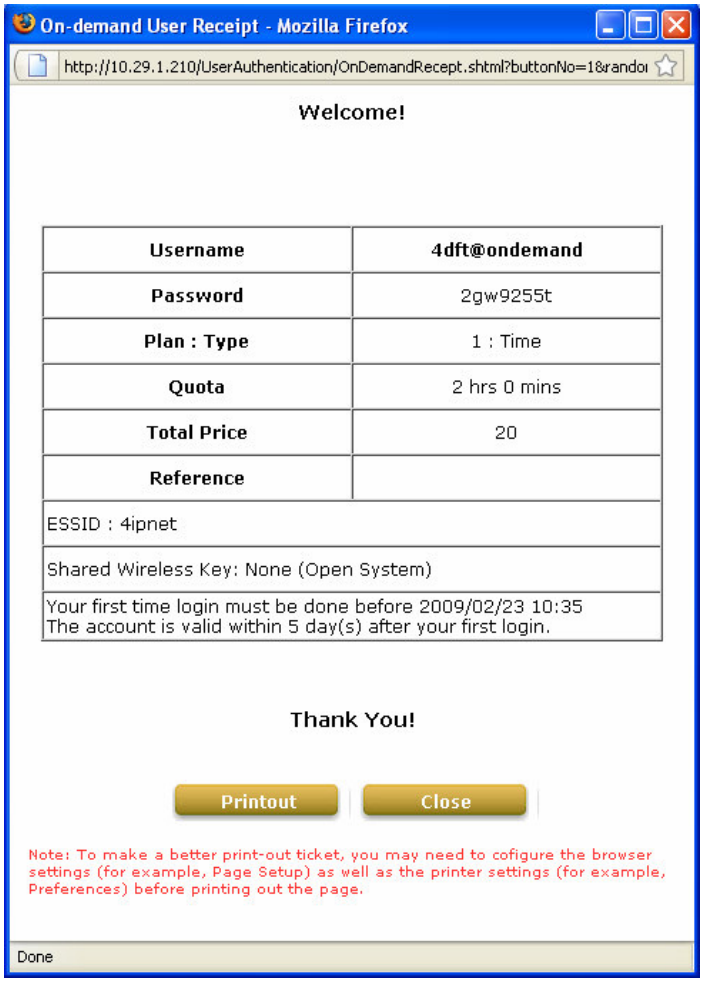


On-demand Account Creation					
Plan	Type	Quota	Price	Status	Function
1	Time	2 hrs 0 mins	20	Enabled	Create

Creating an On-demand Account	
Plan : Type	1 : Time
Quota	2 hrs 0 mins
Account Activation	First time login must be done within 3 day(s)
Valid Period	After activation, the account will be expired in 5 day(s)
Total Price	20
Reference	Add a reference related to this account (for example, the customer's name)
Please confirm the information and press Create button to create an account.	

Create Cancel

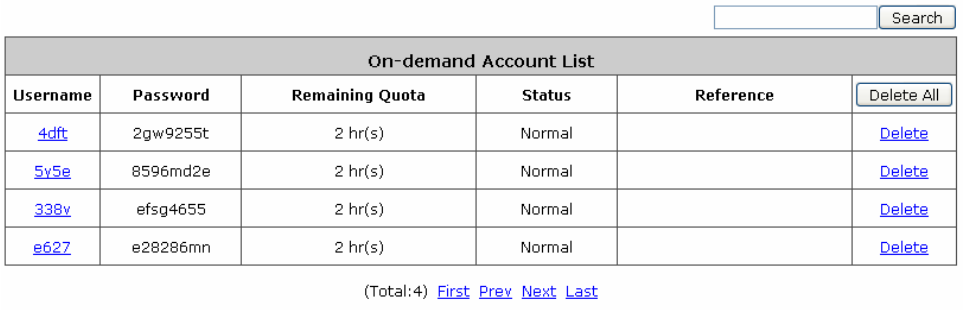
© 2008 4IPNET, INC.


On-demand User Receipt - Mozilla Firefox
http://10.29.1.210/UserAuthentication/OnDemandRecept.shtml?buttonNo=1&rando
Welcome!
Username
4dft@ondemand
Password
2gw9255t
Plan : Type
1 : Time
Quota
2 hrs 0 mins
Total Price
20
Reference
ESSID : 4ipnet
Shared Wireless Key: None (Open System)
Your first time login must be done before 2009/02/23 10:35
The account is valid within 5 day(s) after your first login.
Thank You!
Printout
Close
Note: To make a better print-out ticket, you may need to cofigure the browser settings (for example, Page Setup) as well as the printer settings (for example, Preferences) before printing out the page.
Done

© 2008 4IPNET, INC.

6) On-demand Account List

All created On-demand accounts are listed and related information on is also provided.

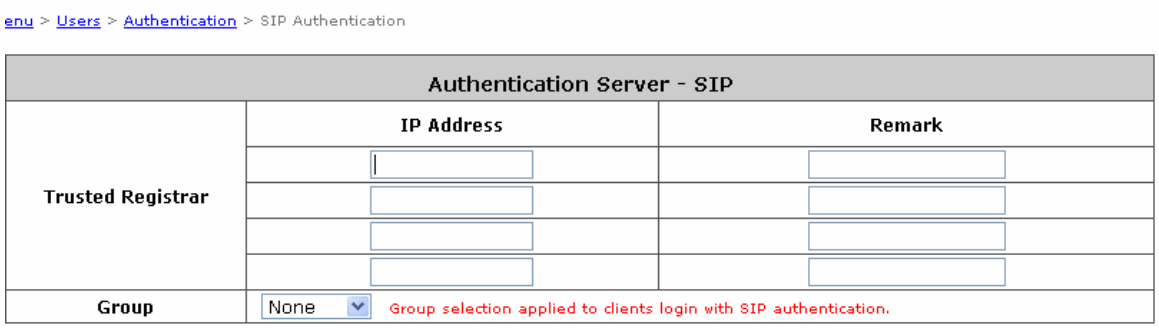


- **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.
- **Username:** The login name of the user.
- **Password:** The login password of the user.
- **Remaining Quota:** The remaining time or volume that the user can continue to use to access the network.
- **Status:** The status of the account.
  - **Normal:** the account is not currently in use and also does not exceed the quota limit.
  - **Online:** the account is currently in use.
  - **Expired:** the account is not valid any more, even there is remaining quota to be used.
  - **Out of Quota:** the account has exceeded the quota limit
  - **Redeemed:** the account has been applied for account renewal.
- **Delete:** This will delete the users individually.

© 2008 4IPNET, INC.

4.2.1.7 Authentication Method – SIP

The system provides SIP proxy for SIP clients (devices or soft clients) pass through NAT. After enable SIP proxy server, all SIP traffic can pass through NAT with a selective but fixed WAN interface.
Administrator will be able to add trusted SIP Registrars up to four of them. A group can be chosen to govern SIP traffic.

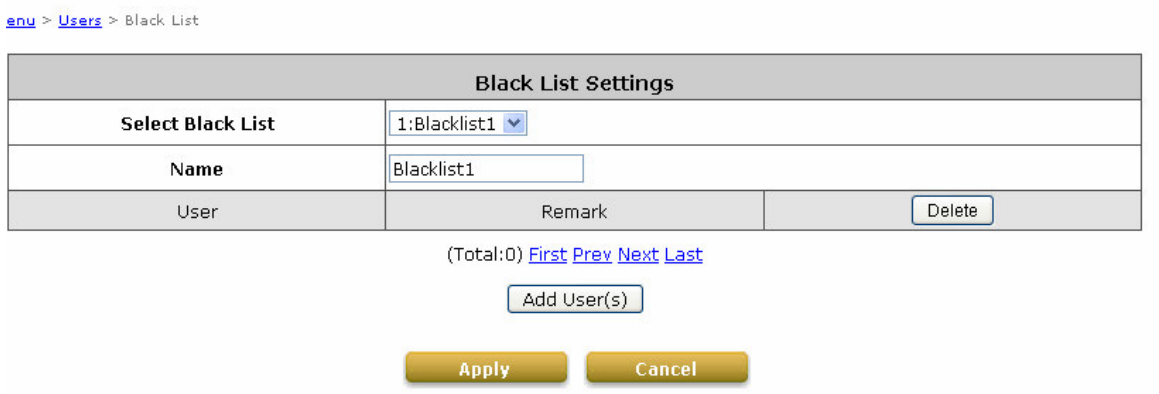


- **SIP:** SIP authentication supports 4 Trusted SIP Registrar.
- **IP Address:** The IP address of the Trusted SIP Registrar.
- **Remark:** The administrator can enter extra information in this field for remark.
- **Group:** A Group option can be applied to the clients who login with SIP Authentication. Be noted that the specific route of the applied Policy for the selected Group cannot conflict with the assigned WAN interface for SIP authentication.

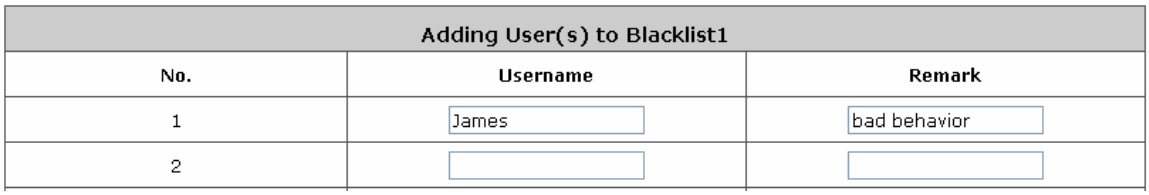
© 2008 4IPNET, INC.

4.2.2 Black List Configuration

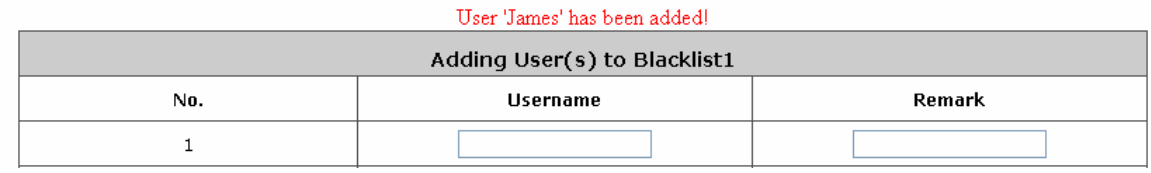
The administrator can add, delete, or edit the black list for user access control. Each black list can include up to 40 users. Users' accounts that appear in the black list will be denied of network access. The administrator can use the drop-down menu to select the desired black list.



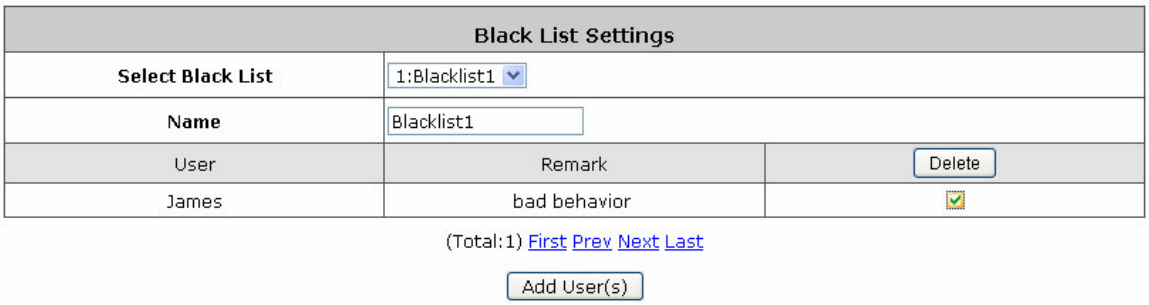
- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the drop-down menu above.
- **Add User to List:** Click the hyperlink to add users to the selected black list.



After entering the usernames in the **"Username"** field blanks and the related information in the **"Remark"** field blank (not required), click ***Apply*** to add the users.



If removing a user from the black list is desired, select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.



© 2008 4IPNET, INC.

4.2.3 Group Configuration

There are 8 groups to choose from. Local users can be classified by applying Group options. A Group which is allowed to access a Service Zone can be applied with a Policy within this zone. The same Group within different Service Zones can be applied with different Policies as well as different Authentication Options.

Group Configuration - Group 1			
Select Group	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	**Enabled**	**Policy**	**To Group Permission Configuration**
Service Zone : Default	☑	Policy 1	Default
Service Zone : SZ1	☑	Policy 1	SZ1
Service Zone : SZ2	☑	Policy 1	SZ2
Service Zone : SZ3	☑	Policy 1	SZ3
Service Zone : SZ4	☑	Policy 1	SZ4
Service Zone : SZ5	☑	Policy 1	SZ5
Service Zone : SZ6	☑	Policy 1	SZ6
Service Zone : SZ7	☑	Policy 1	SZ7
Service Zone : SZ8	☑	Policy 1	SZ8
Remote VPN	☑	Policy 1	Remote VPN

Apply Clear

- **Group Configuration – Group 1~8**
  - **QoS Profile:** Set parameters for traffic classification.

Group 1 - Traffic Configuration	
Traffic Class	Best Effort
Group Total Downlink	Unlimited
Individual Maximum Downlink	Unlimited
Individual Request Downlink	None
Group Total Uplink	Unlimited
Individual Maximum Uplink	Unlimited
Individual Request Uplink	None

© 2008 4IPNET, INC.

- **Traffic Class:** A Traffic Class can be chosen for a Group of users. There are four traffic classes: ***Voice***, ***Video***, ***Best-Effort*** **and** ***Background***. Voice and Video traffic will be placed in the high priority queue. When Best-Effort or Background is selected, more bandwidth management options such as Downlink and Uplink Bandwidth will appear.
- **Group Total Downlink:** Defines the maximum bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Downlink:** Defines the maximum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Downlink cannot exceed the value of Group Total Downlink.
- **Individual Request Downlink:** Defines the guaranteed minimum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.
- **Group Total Uplink:** Defines the maximum uplink bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Uplink:** Defines the maximum uplink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Uplink cannot exceed the value of Group Total Uplink.
- **Individual Request Uplink:** Defines the guaranteed minimum bandwidth allowed for an individual client belonging to this Group. The Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

➢ **Privilege Profile:**

- **Change Password Privilege:** When **Change Password Privilege** is enabled, the authenticated local users within this Group are allowed to change their password via the Login Success Page.

- **Zone Permission Configuration & Policy Assignment – Group 1~8**

  A Group can be assigned to one Service Zone or multiple Service Zones. Moreover, a Group can be applied with different Policies within different Service Zones. Remote VPN is considered as a zone, where clients log into the system via remote VPN.

© 2008 4IPNET, INC.

Group Configuration - Group 1			
Select Group:	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Name	**Enabled**	**Policy**	**Edit Group Permission**
Service Zone : Default	☑	Policy 1	Default
Service Zone : SZ1	☑	Policy 1	SZ1
Service Zone : SZ2	☑	Policy 1	SZ2
Service Zone : SZ3	☑	Policy 1	SZ3
Service Zone : SZ4	☑	Policy 1	SZ4
Service Zone : SZ5	☑	Policy 1	SZ5
Service Zone : SZ6	☑	Policy 1	SZ6
Service Zone : SZ7	☑	Policy 1	SZ7
Service Zone : SZ8	☑	Policy 1	SZ8
Remote VPN	☑	Policy 1	Remote VPN

- **Name:** The name of Service Zones and Remote VPN.
- **Enabled:** Select *Enabled* to allow clients of this Group to log into the selected Service Zones. For example, the above figure shows that users in Group 1 can access network services via every Service Zone as well as Remote VPN under constraints of Policy 1.
- **Policy:** Select a *Policy* that the Group will be applied with when accessing respective Service Zones.
- **Edit Group Permission:** The relation between Group and Service Zone is many to many; every Group can access network services via more than one Service Zone, and meanwhile, each Service Zone can serve more than one Group.

Click the hyperlink in the **Edit Group Permission** column to enter the **Group Configuration** interface, which is based on the role of Service Zone, to configure the relation between Group and Zone.

© 2008 4IPNET, INC.

Group Permission - Service Zone : Default			
Group Option	Enabled	Policy	Edit Group Option
Group 1	☑	Policy 1	Group 1
Group 2	☑	Policy 2	Group 2
Group 3	☑	Policy 3	Group 3
Group 4	☑	Policy 4	Group 4
Group 5	☑	Policy 5	Group 5
Group 6	☑	Policy 6	Group 6
Group 7	☑	Policy 7	Group 7
Group 8	☑	Policy 8	Group 8

- **Group Option:** The name of Group options available for selection.
- **Enabled:** Select *Enabled* to allow clients of the enabled Groups to log in to this Service Zone under constraints of the selected Policies.
  Check *Enabled* of each individual Group to assign it to the Service Zone listed. For example, the above figure shows, clients in Group 1~8 can access Default Service Zone, where they are governed by Policy 1~8 respectively.
- **Policy:** Select a *Policy* that the Group will be applied with when accessing this Service Zone.
- **Edit Group Option:** Click the hyperlink in the **Edit Group Option** column to enter **Zone Permission Configuration & Policy Assignment** interface, which is based on the role of Group, to configure the relation between Group and Zone.

© 2008 4IPNET, INC.

4.2.4 Policy Configuration

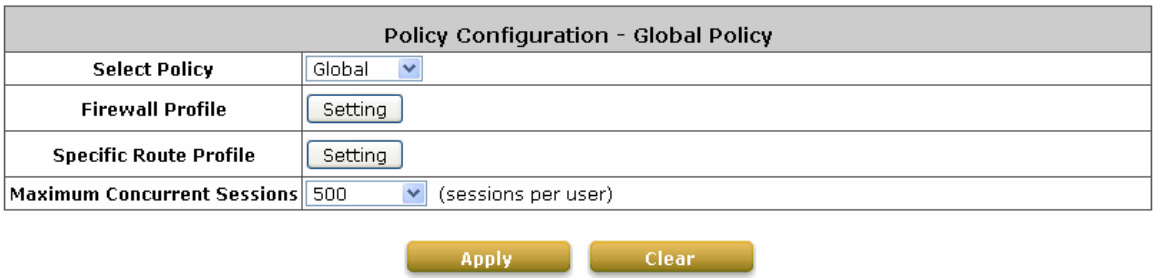
WHG303 supports multiple Policies, including one **Global Policy** and 12 individual **Policy**. Each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. **Global Policy** is the system's universal policy and applied to all clients, while other individual Policy can be selected and defined to be applied to any Service Zone.

The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.

When the type of authentication database is RADIUS, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a RADIUS class attribute. When the type of authentication database is LDAP, the **Attribute-Group Mapping** function will be available to allow the administrator to assign a Group for LDAP attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a LDAP attribute. When the type of database is SIP, the **Group** selection function will be available to allow the administrator to assign a Group option for all SIP clients.

4.2.4.1 Global Policy

Global is the system's universal policy including **Firewall Rules**, **Specific Routes Profile** and **Maximum Concurrent Session** which will be applied to all users unless the user has been regulated and applied with another Policy.



- **Select Policy:** Select **Global** to set the **Firewall Profile**, **Specific Route Profile** and **Privilege Profile**.
- **Firewall Profile:** Global policy and each policy have a firewall service list and a set of firewall profile which is composed of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

© 2008 4IPNET, INC.

- **Firewall Profile:** Click ***Setting*** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.

  - **Predefined and Custom Service Protocols:** There are predefined service protocols available for firewall rules editing. The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols with ***Select All*** and ***Delete*** operations.
    This link leads to a Service Protocols List where the administrator can define a list of service by protocols (TCP/UDP/ICMP/IP).

Global Policy - Service Protocols List

No.	Name	Description	Select All
1	ALL	ALL	☐
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
4	ALL ICMP	ICMP; Type: Any, Code: Any	☐
5	FTP	TCP/UDP; Destination Port: 20;21	☐
6	HTTP	TCP/UDP; Destination Port: 80	☐
7	HTTPS	TCP/UDP; Destination Port: 443	☐
8	POP3	TCP; Destination Port: 110	☐
9	SMTP	TCP; Destination Port: 25	☐
10	DHCP	UDP; Destination Port: 67;68	☐

Add Delete

(Total: 27) First Prev Next Last

  - **Firewall Rules:** Click the number of ***Filter Rule No.*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **"Active"** box and click ***Apply*** to enable that rule. This link leads to the Firewall Rules page. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by Source, Destination and Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to Always, Recurring or One Time.

© 2008 4IPNET, INC.

Global Policy - Firewall Rules							
No.	Active	Action	Name	Source Destination	IPSec Encrypted IPSec Encrypted	Service	Schedule
1	☐	Block		ANY ANY		ALL	Always
2	☐	Block		ANY ANY		ALL	Always

Selecting the Filter Rule Number 1 as an example:

Global Policy - Edit Filter Rule			
Rule Item	1		
Rule Name			
Source		Destination	
Interface	ALL	Interface	ALL
IP Address	0.0.0.0	IP Address	0.0.0.0
Subnet Mask	0.0.0.0 (/0)	Subnet Mask	0.0.0.0 (/0)
IPSec Traffic	☐	IPSec Traffic	☐
MAC Address			
Service	ALL		
Schedule	◉ Always ○ Recurring ○ One Time		
Action	◉ Block ○ Pass		

- **Rule Number:** This is the rule selected "1". Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source/Destination – Interface/Zone:** There are choices of **ALL, WAN1**, **WAN2**, **Default**, and the named **Service Zones** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Host filtering is supported but Domain name filtering is not.
- **Source/Destination – Subnet Mask:** Select the source and destination subnet masks.
- **Source- MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
- **Source/Destination – IPSec Encrypted:** Check the box for only filtering on the encrypted traffic.
- **Service Protocol:** There are defined protocols in the **service protocols list** to be selected.
- **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time.** **Recurring** is set with the hours within a week.

© 2008 4IPNET, INC.

- **Action for Matched Packets:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

➢ **Specific Route Profile:** Click the button of ***Setting*** for **Specific Route Profile**, the Specific Route Profile list will appear.

Global Policy - Specific Route Profile			
Route Item	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	

- **Route No.:** The number of route.
- **IP Address (Destination):** The destination IP address of the host or the network.
- **Subnet Netmask:** Select a destination subnet netmask of the host or the network.
- **IP Address (Gateway):** The IP address of the next router to the destination.

➢ **Maximum Concurrent Session for User:** Include Maximum Concurrent Session for User, from 10 to Unlimited. The concurrent sessions for each user, it can be restricted by administrator.

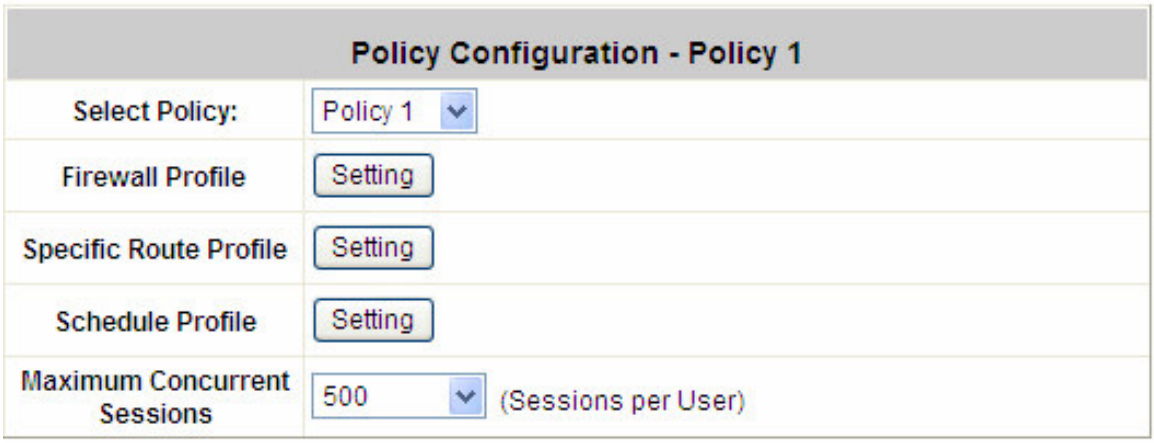
Note: For more information, please refer to **Appendix F. Session Limit and Session Log**.

© 2008 4IPNET, INC.

4.2.4.2 Policy 1 ~ Policy 12

Each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.

When the type of authentication database is RADIUS, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a RADIUS class attribute. When the type of authentication database is LDAP, the **Attribute-Group Mapping** function will be available to allow the administrator to assign a Group for LDAP attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a LDAP attribute. When the type of database is SIP, the **Group** selection function will be available to allow the administrator to assign a Group option for all SIP clients.



- **Select Policy:** Select **Policy1~Policy12** to set the **Firewall Profile**, **Specific Route Profile, Schedule Profile** and **Maximum Concurrent Session**.
- **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profile consisting of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied policies are only allowed to login the system at the time which is checked in the applied policy.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

  - **Firewall Profile:** Click ***Setting*** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.

© 2008 4IPNET, INC.

Policy 1 - Firewall Configuration
Predefined and Custom Service Protocols
Firewall Rules

- **Predefined and Custom Service Protocols:** This link leads to a Service Protocols List where the administrator can define a list of service by protocols (TCP/UDP/ICMP/IP). There are predefined service protocols available for firewall rules editing. The administrator is able to add new customized service protocols by clicking ***Add***, and delete the added protocols by clicking ***Delete***.

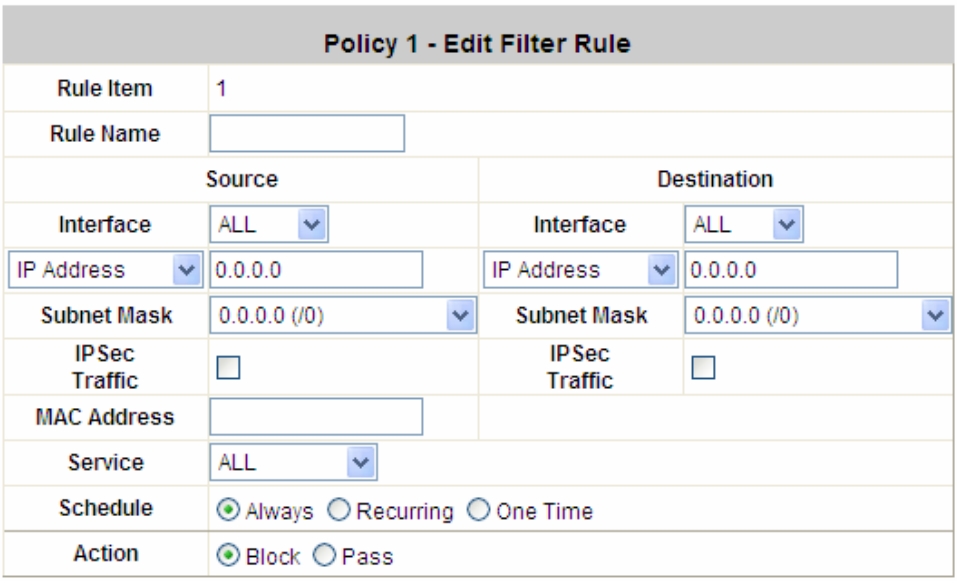
Global Policy - Service Protocols List			
No.	**Name**	**Description**	Select All
1	ALL	ALL	☐
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
4	ALL ICMP	ICMP; Type: Any, Code: Any	☐
5	FTP	TCP/UDP; Destination Port: 20;21	☐
6	HTTP	TCP/UDP; Destination Port: 80	☐
7	HTTPS	TCP/UDP; Destination Port: 443	☐
8	POP3	TCP; Destination Port: 110	☐
9	SMTP	TCP; Destination Port: 25	☐
10	DHCP	UDP; Destination Port: 67;68	☐
		Add Delete	
		(Total: 27) First Prev Next Last	

- **Firewall Rules:** Click on the hyperlink in the **No.** column to edit individual rules and then click ***Apply*** to save the settings. The rule status will show on the list. Check the *Active* check box and click ***Apply*** to enable that rule. This link leads to the **Firewall Rules** page. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by **Source**, **Destination** and **Pass**/**Block** action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to *Always*, *Recurring* or *One Time*.

Policy 1 - Firewall Rules							
No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☐	Block		ANY		ALL	Always
				ANY			
2	☐	Block		ANY		ALL	Always
				ANY			

Below depicts an example of selecting Filter Rule Number 1:

© 2008 4IPNET, INC.



- **Rule Item:** This rule number of the selected rule. Rule No. 1 has the highest priority; Rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source / Destination – Interface/Zone**: There are choices of *ALL*, *WAN1*, *WAN2*, *Default* and the *Service Zones* to be applied to the traffic interface.
- **Source / Destination – IP Address/Domain Name:** Enter the source and destination IP addresses.
- **Source / Destination – Subnet Mask:** Enter the source and destination subnet masks.
- **Source / MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
- **Source / Destination – IPSec Traffic:** Check the box to filter the encrypted traffic only.
- **Service Protocol:** Select a defined protocol from the drop-down list box.
- **Schedule:** Defines the time when this firewall rule will be activated. When a schedule is selected, the clients assigned to this Policy are applied with the firewall rule only within the time selected. There are three options, *Always*, *Recurring* and *One Time*.
- **Action for Matched Packets:** There are two options, *Block* and *Pass*. Block is to prevent packets from passing, while Pass is to permit packets passing.

➢ **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a Policy. When Specific Default Route is enabled, all clients applied with this Policy will access the Internet through this default gateway.

© 2008 4IPNET, INC.

Policy 1 - Specific Default Route			
Enable ☐	Default Gateway:	IP Address	

Policy 1 - Specific Routes			
Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	
3		255.255.255.255 (/32)	

Click ***Setting*** of *Specific Route Profile* to enter the **Specific Route** page for further configuration.

- **Enable:** Check ***Enable*** box to activate this function or uncheck to inactivate it.
- **Destination** / **IP Address:** The destination network address or IP address of the destination host. Please note that, if applicable, the system will calculate and display the appropriate value based on the combination of Network/IP Address and Subnet Mask that are just entered and applied.
- **Destination** / **Subnet Netmask:** The subnet mask of the destination network. Select *255.255.255.255(/32)* if the destination is a single host.
- **Gateway** / **IP Address:** The IP address of the gateway or next router to the destination.

➢ **Schedule Profile:** Click ***Setting*** of *Schedule Profile* to enter the configuration page. Select ***Enable*** to show the **Permitted Login Hours** list. This function is used to limit the time when clients can log in. Check the desired time slots and click ***Apply*** to save the settings. These settings will become effective immediately after clicking ***Apply***.

◉ Enable ○ Disable

Policy 1 - Permitted Login Hours							
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
00:00~00:59	☑	☑	☑	☑	☑	☑	☑
01:00~01:59	☑	☑	☑	☑	☑	☑	☑
02:00~02:59	☑	☑	☑	☑	☑	☑	☑
03:00~03:59	☑	☑	☑	☑	☑	☑	☑
04:00~04:59	☑	☑	☑	☑	☑	☑	☑
05:00~05:59	☑	☑	☑	☑	☑	☑	☑
06:00~06:59	☑	☑	☑	☑	☑	☑	☑
07:00~07:59	☑	☑	☑	☑	☑	☑	☑
08:00~08:59	☑	☑	☑	☑	☑	☑	☑
09:00~09:59	☑	☑	☑	☑	☑	☑	☑
10:00~10:59	☑	☑	☑	☑	☑	☑	☑

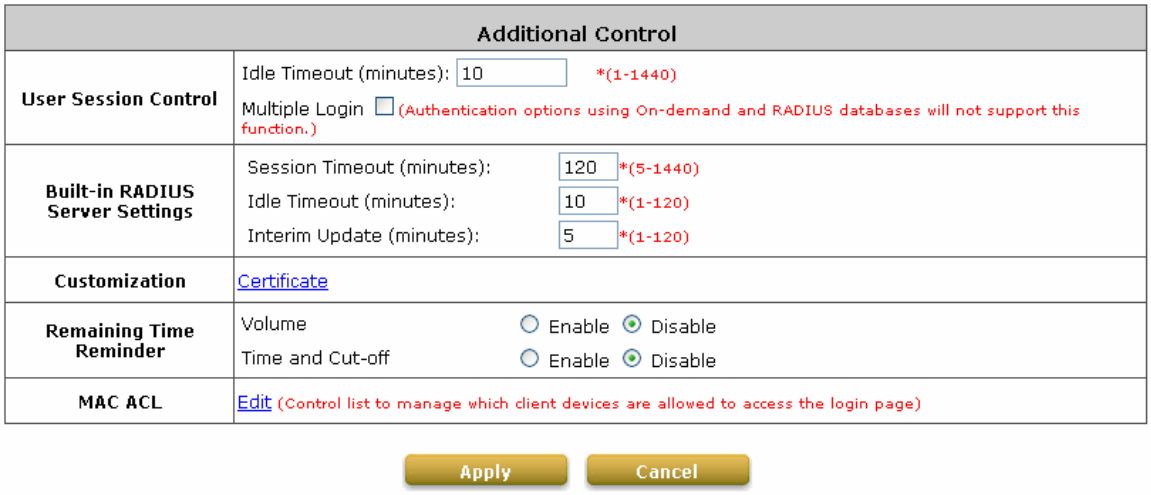
➢ **Maximum Concurrent Session for User:** Include Maximum Concurrent Session for User, from 10 to Unlimited. The concurrent sessions for each user, it can be restricted by administrator.

© 2008 4IPNET, INC.

Note: For more information, please refer to **Appendix F. Session Limit and Session Log**.

© 2008 4IPNET, INC.

4.2.5 Additional Configuration


Additional Control
User Session Control
Idle Timeout (minutes): 10 *(1-1440)
Multiple Login (Authentication options using On-demand and RADIUS databases will not support this function.)
Built-in RADIUS Server Settings
Session Timeout (minutes): 120 *(5-1440)
Idle Timeout (minutes): 10 *(1-120)
Interim Update (minutes): 5 *(1-120)
Customization
Certificate
Remaining Time Reminder
Volume Enable Disable
Time and Cut-off Enable Disable
MAC ACL
Edit (Control list to manage which client devices are allowed to access the login page)
Apply
Cancel

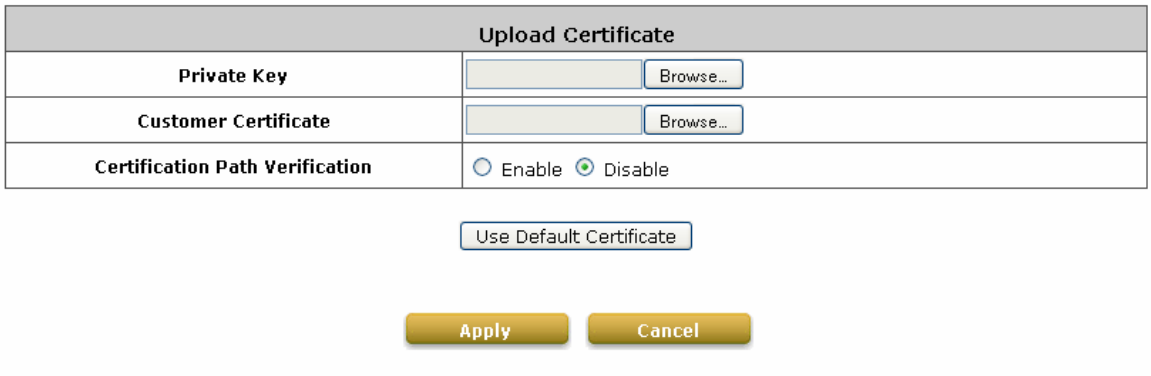
- **User Control:** Functions under this section apply to all general users.
  Idle Timer: If a user has idled with no network activities, the system will automatically kick out the user. The logout timer can be set between 1~1440 minutes, and the default logout time is 10 minutes.
  Multiple Login: When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS authentication.)

- **Roaming Out Timer**
  Session Timeout: The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.
  Idle Timeout: If a user has idled with no network activities, the system will automatically kick out the user.
  Interim Update: The system will update the users' current status and usage according to this time period.

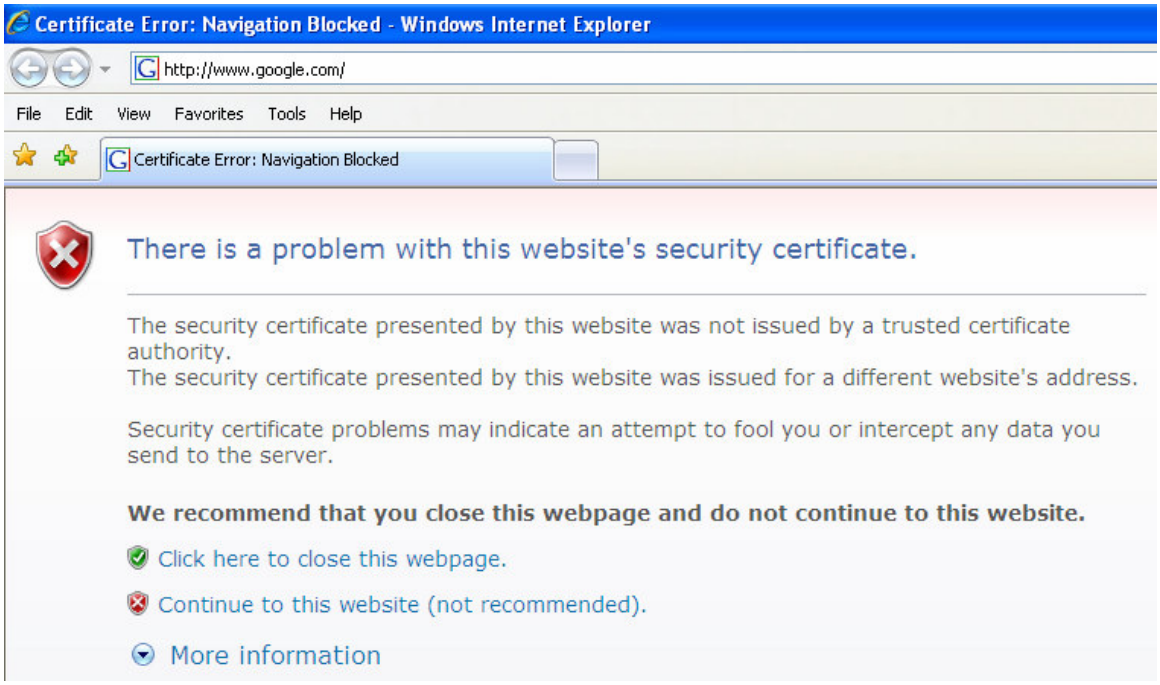
- **Upload File**
  Certificate: A data record used for authenticating network entities such as a server or a client. A certificate contains X.509 information pieces about its owner (called the subject) and the signing Certificate Authority (called the issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates. You can apply for a SSL certificate at CAs such as VeriSign.

  If you already have an SSL Certificate, please Click Browse to select the file and upload it. Click ***Apply*** to complete the upload process.

© 2008 4IPNET, INC.

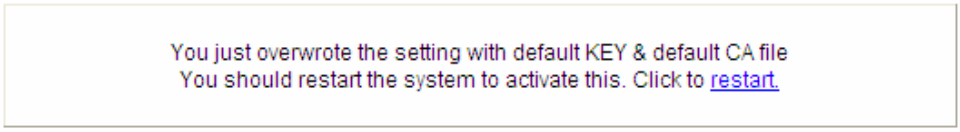


Without a valid certificate, users may encounter the following problem in IE7 when they try to open the login page.


Certificate Error: Navigation Blocked - Windows Internet Explorer
http://www.google.com/
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Click "Continue to this website" to access the user login page.

To Use Default Certificate: Click ***Use Default Certificate*** to use the default certificate and key. Click **restart** to validate the changes.


You just overwrote the setting with default KEY & default CA file
You should restart the system to activate this. Click to restart.

- **Remaining Time Reminder:** The administrator can enable this function to remind the on-demand users before their credit run out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.

© 2008 4IPNET, INC.

Remaining Time Reminder	Volume	○ Enable ◉ Disable
	Time and Cut-off	○ Enable ◉ Disable

- **MAC ACL:** With this function, only the users with their MAC addresses in this list can log into WHG303. There are 100 users maximum allowed in this MAC address list. User authentication is still required for these users. Please enter the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click ***Apply***.

Access Control List			
○ Enable ◉ Disable			
No.	**MAC Address**	**No.**	**MAC Address**
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

(Total:100) First Prev Next Last

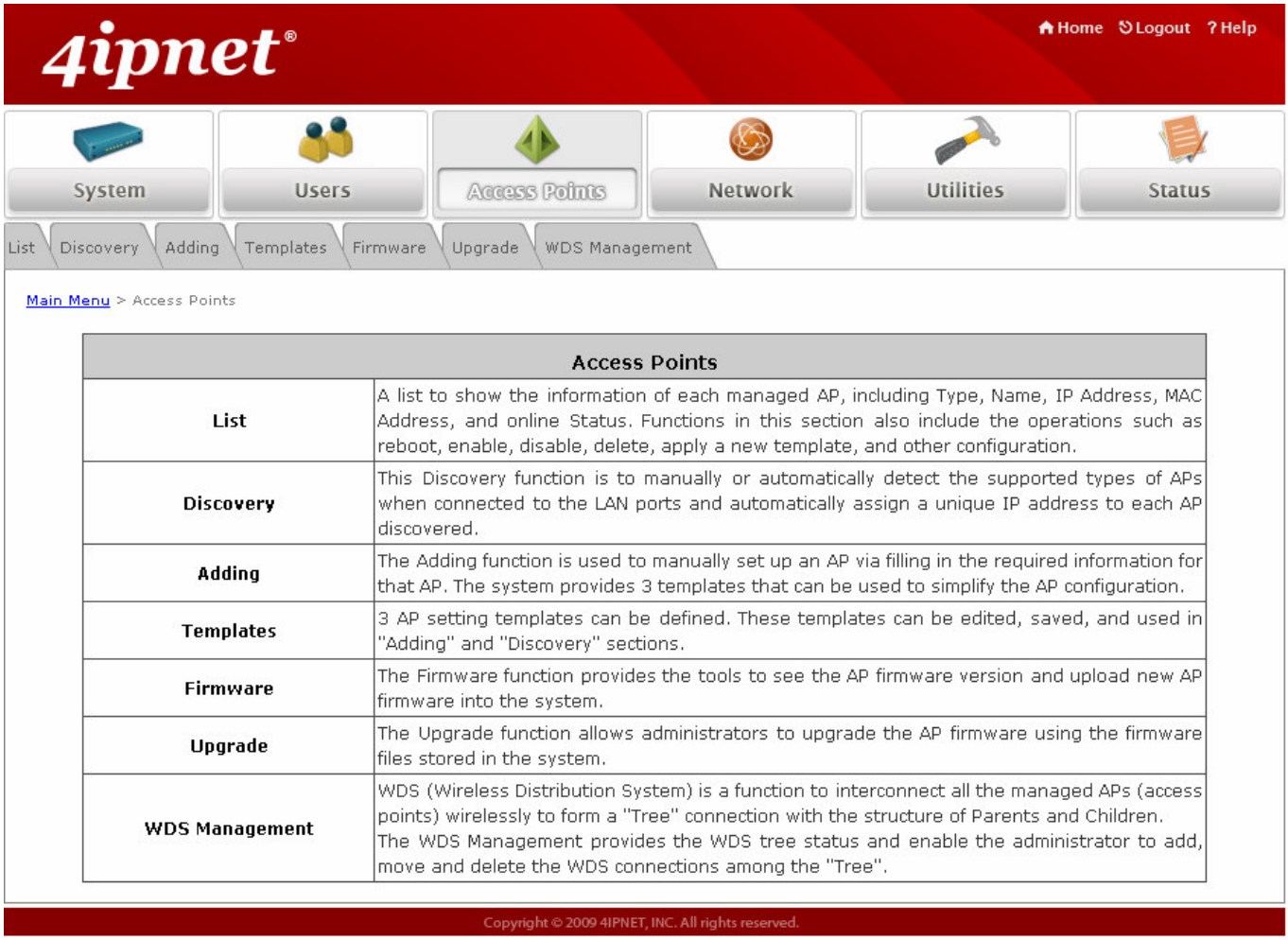
Apply Cancel

The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

© 2008 4IPNET, INC.

4.3 AP Management

WHG303 supports to manage up to 20 access points (AP), and they can be configured in this section. This section includes the following functions: **AP List**, **AP Discovery**, **Adding APs**, **Template Selection**, **Firmware Upload, AP Upgrade** and **WDS Management**.

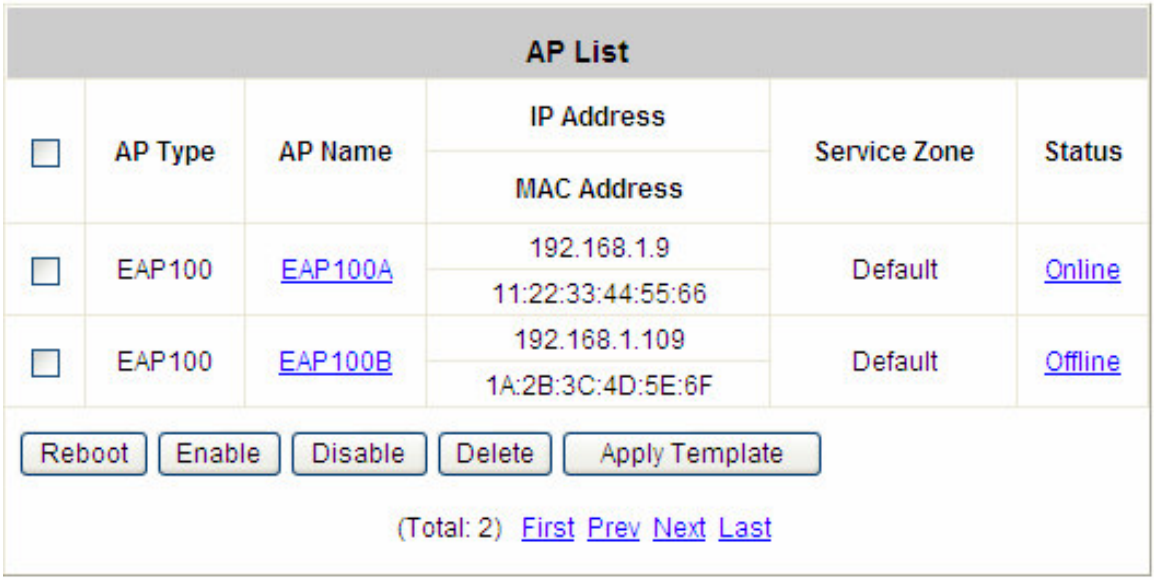


Access Points	
List	A list to show the information of each managed AP, including Type, Name, IP Address, MAC Address, and online Status. Functions in this section also include the operations such as reboot, enable, disable, delete, apply a new template, and other configuration.
Discovery	This Discovery function is to manually or automatically detect the supported types of APs when connected to the LAN ports and automatically assign a unique IP address to each AP discovered.
Adding	The Adding function is used to manually set up an AP via filling in the required information for that AP. The system provides 3 templates that can be used to simplify the AP configuration.
Templates	3 AP setting templates can be defined. These templates can be edited, saved, and used in "Adding" and "Discovery" sections.
Firmware	The Firmware function provides the tools to see the AP firmware version and upload new AP firmware into the system.
Upgrade	The Upgrade function allows administrators to upgrade the AP firmware using the firmware files stored in the system.
WDS Management	WDS (Wireless Distribution System) is a function to interconnect all the managed APs (access points) wirelessly to form a "Tree" connection with the structure of Parents and Children. The WDS Management provides the WDS tree status and enable the administrator to add, move and delete the WDS connections among the "Tree".

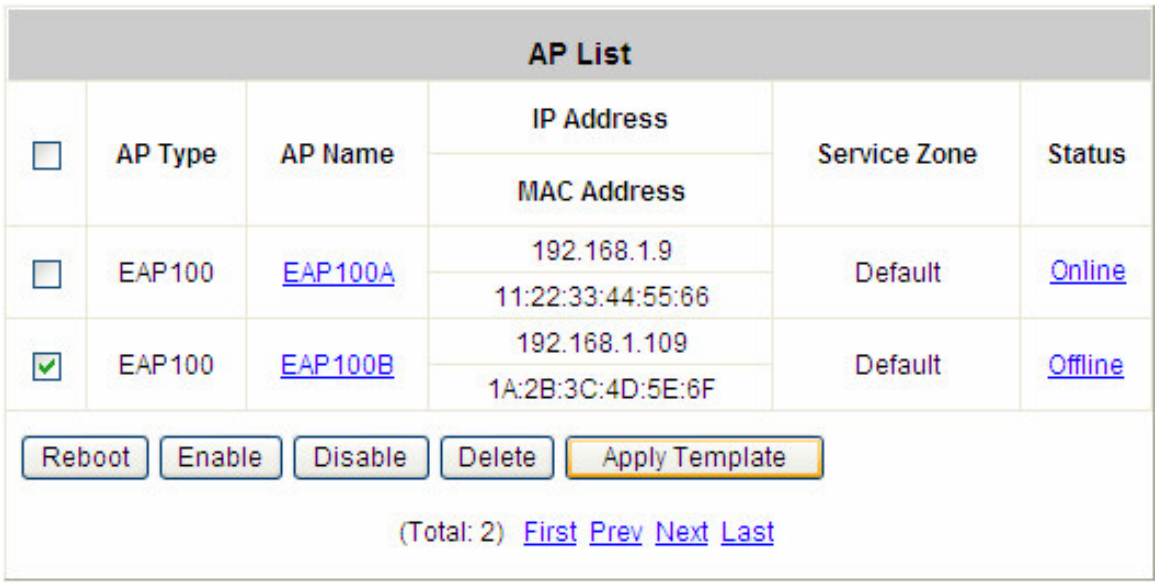
© 2008 4IPNET, INC.

4.3.1 AP List

All of the APs under the management of WHG303 will be shown in the list. The AP can be edited by clicking the hyperlink of ***AP Name*** and the AP status can be got by clicking the hyperlink of ***Status***.

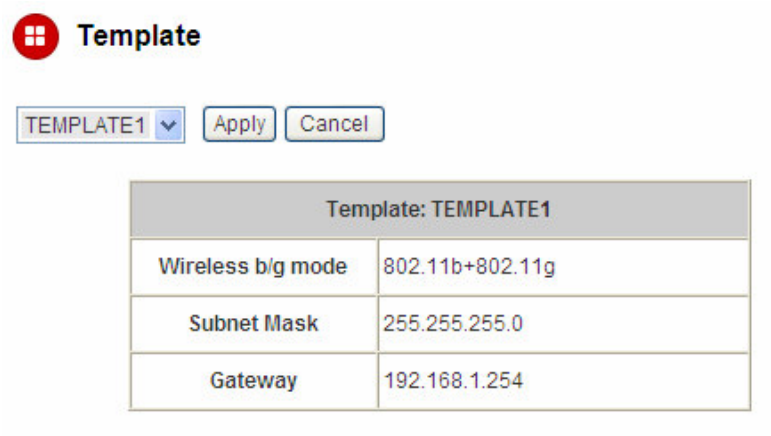


Check any AP and then click the button below to ***Reboot***, ***Enable***, ***Disable*** and ***Delete*** the checked AP if desired.



Click ***Apply Template*** to select one template to apply to the AP.

© 2008 4IPNET, INC.



© 2008 4IPNET, INC.

- **AP Name**

  Click ***AP Name*** and enter the interface about related settings. There are four kinds of settings, **General Settings**, **LAN Interface Setting**, **Wireless Interface Setting** and **Access Control Setting**. Click the hyperlink to go on the configuration.

General Settings		
General	Name	EAP100B
	Firmware	1.00

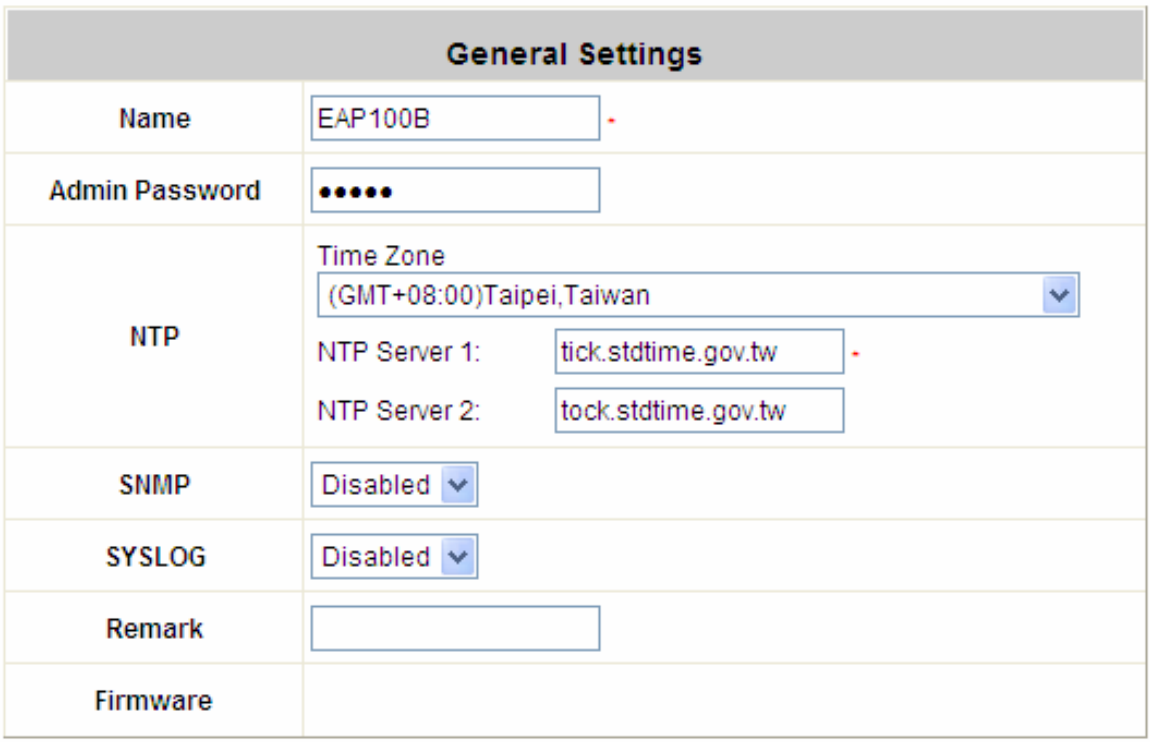
LAN Interface Settings		
LAN	IP	192.168.1.109
	Gateway	192.168.1.254

Wireless Interface Settings		
Wireless LAN	Channel	Auto
	Data Rate	Auto

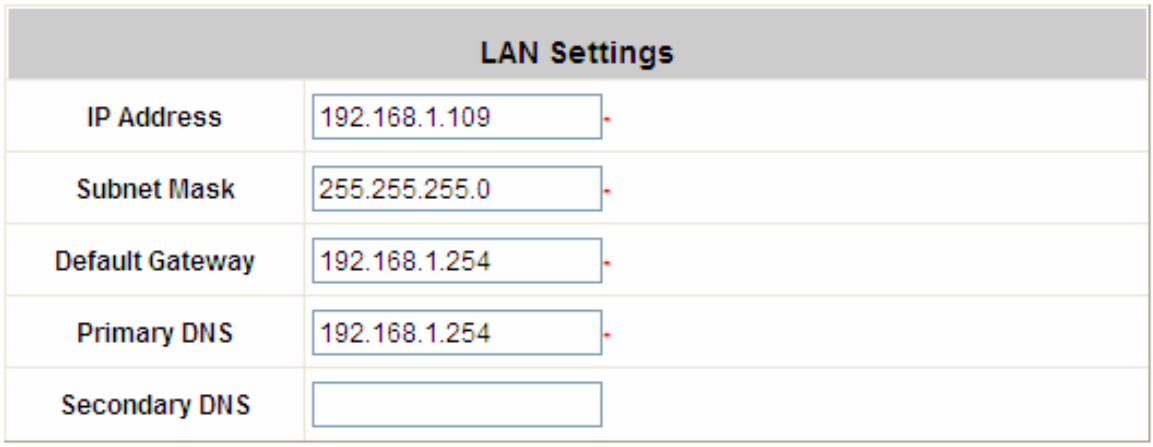
Access Control Settings		
Access Control	Status	Disabled
	Number of MAC Addresses	0

  - **General Setting:** Click ***Setting*** to enter the **General Setting** interface. Firmware information can be observed here.

© 2008 4IPNET, INC.



- **LAN Setting:** Click ***LAN*** to enter the **LAN Setting** interface. Input the data of LAN including **IP address**, **Subnet Mask** and **Default Gateway** of AP.



  - **Wireless LAN:** Click ***Wireless LAN*** to enter the **Wireless** interface.

- **Access Control:** In this function, when the status is **"Allowed"**, only these clients whose MAC addresses are listed in this list can be allowed to connect to the AP; on the other hand, when the status is "Denied", the clients whose MAC addresses are listed in the list will be denied to connect to the AP. When **"Disabled"** is selected, all clients can connect to the AP. The default is **Disabled**.
  - **User Limit:** Limit the number of users connected to that AP.

© 2008 4IPNET, INC.

Access Control	
Status	Allowed
User Limit	32 (Range: from 1 to 32)

MAC Address List			
12:13:14:1A:1B:1C	Disabled		Disabled
	Disabled		Disabled
	Disabled		Disabled
	Disabled		Disabled
	Disabled		Disabled

© 2008 4IPNET, INC.

- **Status**

  After clicking the hyperlink in the Status column, there are two areas of information shown: **AP Status Summary** and **AP Status Details**. AP Status Summary includes **AP Name**, **AP Type**, **LAN Interface MAC address**, **Wireless Interface MAC address**, **Report Time**, **SSID**, and **Number of Associated Clients**. AP Status Details include **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status** **Associated Client Status** and **Local Log Status.**

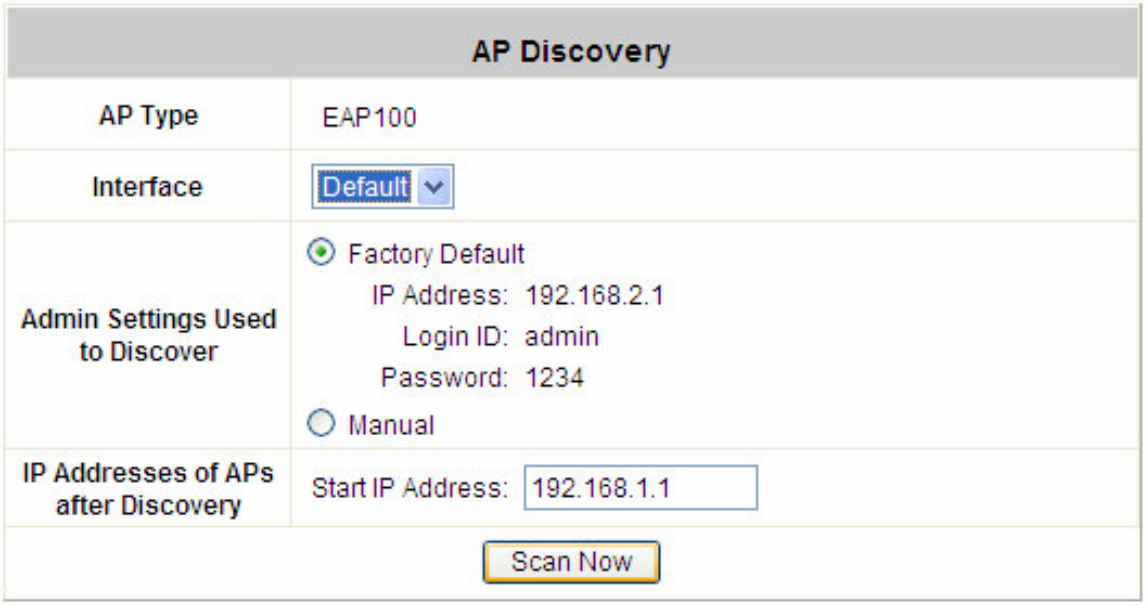
AP Status Summary	
AP Name	EAP100B
AP Type	EAP100
LAN MAC	
Wireless LAN MAC	
Report Time	N/A
SSID	4ipnet (Service Zone: Default)
Number of Associated Clients	0

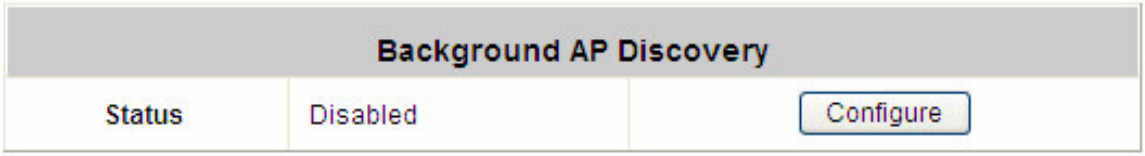
AP Status Detail
System Status
LAN Status
Wireless LAN Status
Access Control Status
Associated Client Status
Local Log Status

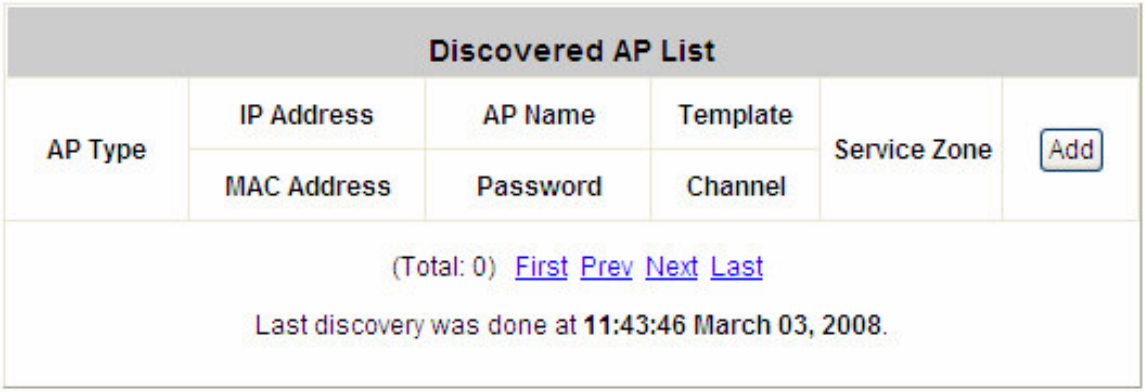
© 2008 4IPNET, INC.

4.3.2 AP Discovery

Use this function to detect and manage all of the APs in the network segments. Note that WHG303 can only manage APs that are connected to its LAN ports. Therefore, the AP discovery function is for adding locally connected APs to its management list. The administrator must know the local IP addresses of the APs he/she wishes to discover.







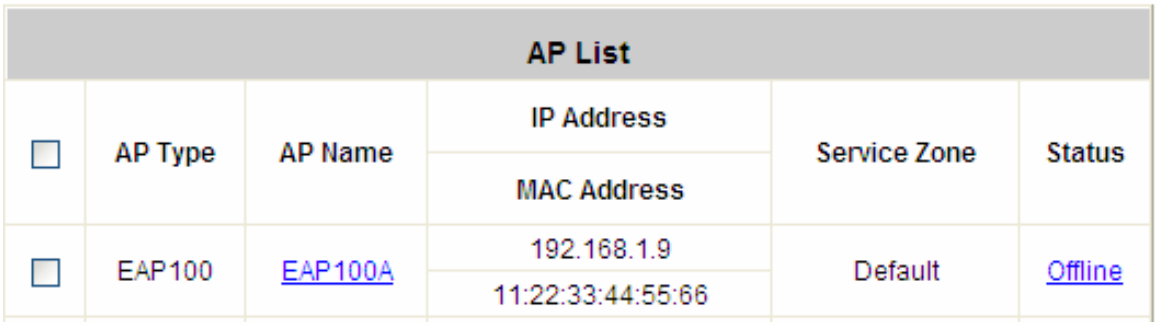
- To discover AP manually, please fill in the required data.
  - **AP Type:** Choose the type of AP you wish to discover.
  - **Interface:** Set to default.
  - **Admin Settings Used to Discover:** Choose from Factory Default or Manual.
  - **IP Addresses of APs after Discovery:** Start assigning from this IP address to discovered APs.

Then click the ***Scan Now*** button and the APs match the given settings will show in the list below. If one of the IP addresses intended is used, a warning message will show up. In this case, please change the IP range and

© 2008 4IPNET, INC.

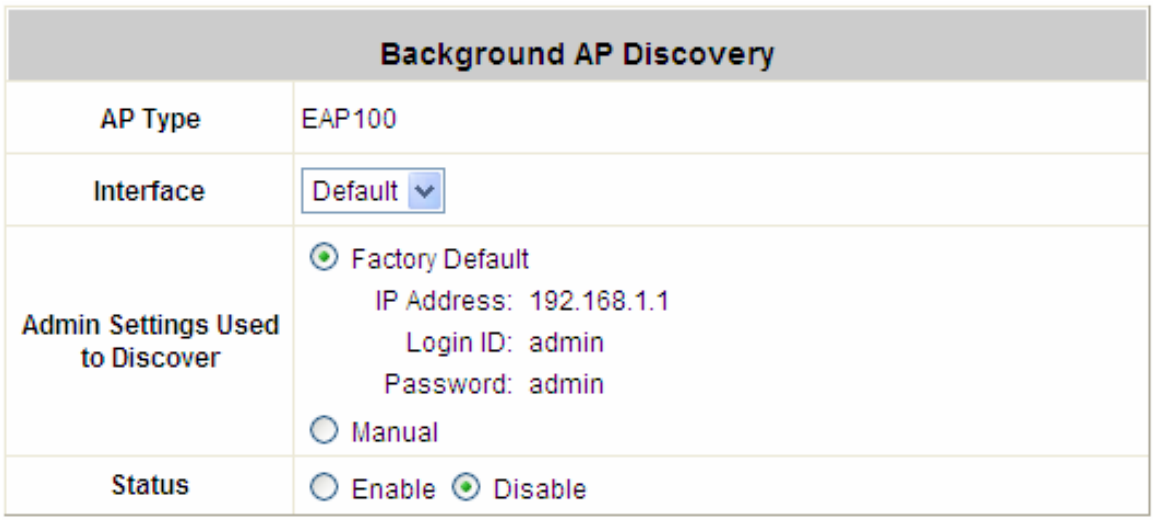
then click ***Scan Now*** again. Input the desired name and password for the AP. Select one template check it and then click ***Add*** to add it under the managed list. (About the template, please see 4.3.4 Template Settings). When the matched AP is discovered, it will show up in the list below and be given a new IP address set here (ex: 192.168.1.1). Check the **Add** box to add the AP and it will be listed to the AP list. When an AP is added, its MAC address will be automatically recorded into MAC Privilege List (please see 4.4.2 Privilege List) so its management page can be accessed.

Click Configuring to go on the related configuration. For the details, please refer to **4.3.1 AP List**.



AP List					
☐	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
☐	EAP100	EAP100A	192.168.1.9 11:22:33:44:55:66	Default	Offline

- **Background AP Discovery:** Click ***Configure*** to enter Background AP Discovery interface to go on related configuration.



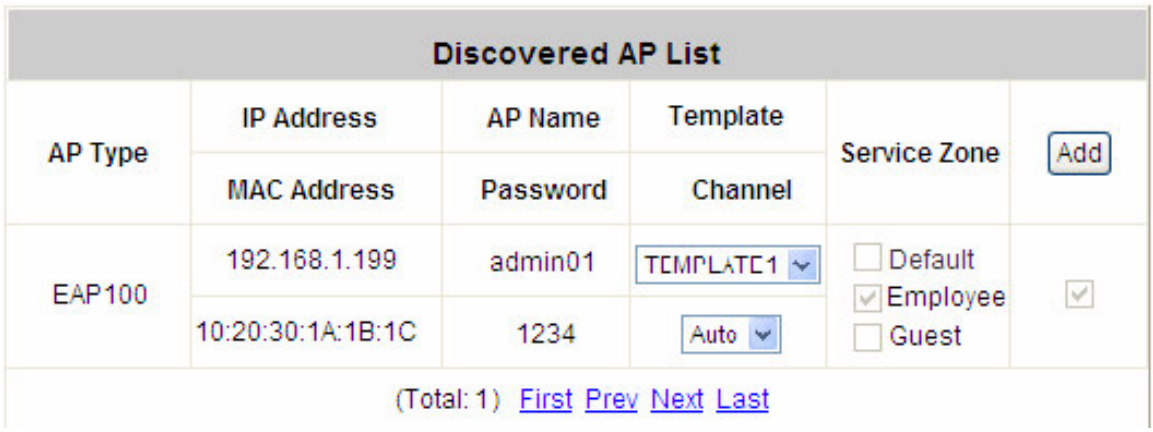
Background AP Discovery	
AP Type	EAP100
Interface	Default
Admin Settings Used to Discover	◉ Factory Default IP Address: 192.168.1.1 Login ID: admin Password: admin ○ Manual
Status	○ Enable ◉ Disable

The **Interface** and **AP Access** configuration is the same as the settings mentioned above. When **Background AP Discovery** function is enabled, the system will scan once every 10 minutes or according to the time set by the administrator. If any AP is discovered and "Auto-Add AP" is enabled, it will be assigned an available IP from the starting IP address and apply the selected template. You can also set the channel the AP would use.

The scanning process may take a long time if the IP range assigned to scan is too wide.

© 2008 4IPNET, INC.

- **Discovered AP List:** The discovered new APs will be listed here. When the system's Service Zone is set to Tag-based mode, service zones also can be assigned here. After clicking ***Add***, the current management page is directed to AP List, where the newly added APs will show up with a status of "configuring". It may take a couple of minutes to see the status of the newly added AP to change from "configuring" to "online" or "offline".

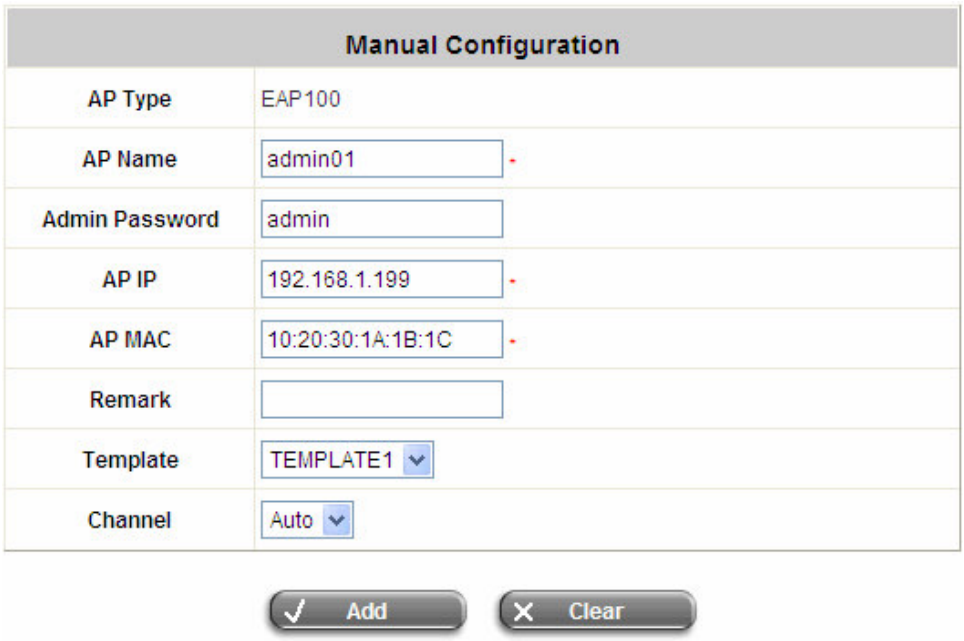


  - **AP Type**: This is the supported type of APs for centralized management.
  - **IP Address:** IP address of the specified AP.
  - **MAC Address:** MAC address of the specific AP.
  - **AP Name:** Mnemonic name of the specific AP.
  - **Admin Password:** Password required for this AP.
  - **Template:** The template which will be applied to the added AP.
  - **Channel:** The selected channel will be applied to the added AP.
  - **Service Zone:** The item is only shown when Tag-Based mode is selected. Select the name of Service Zone such as Service Zone 1, Guest or Employee.
  - **Add:** The administrator can click ***Add*** button to register the APs to the ***List*** for management.

© 2008 4IPNET, INC.

4.3.3 Adding

The AP also can be added manually even though when it is offline. Input the related data of the AP and select a Template. After clicking ***Add***, the AP will be added to the managed list.

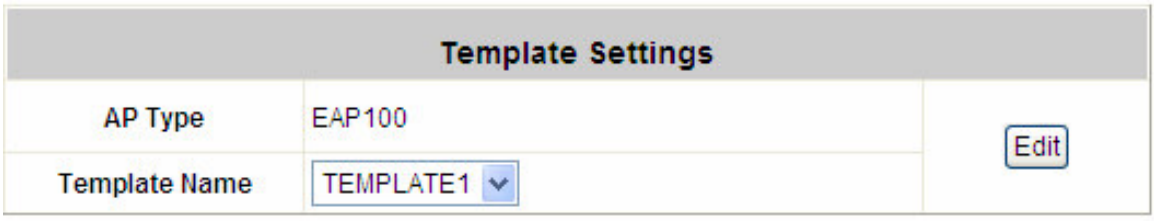


- **AP Type**: This is the supported type of APs for centralized management.
- **AP Name:** Mnemonic name of the specific AP.
- **Admin Password:** Password required for this AP.
- **AP IP:** IP address of the specified AP.
- **AP MAC:** MAC address of the specific AP.
- **Remark:** Some extra information to be filled in for this AP if desired.
- **Template Applied:** The template which will be applied to the added AP.
- **Channel:** The selected channel will be applied to the added AP.

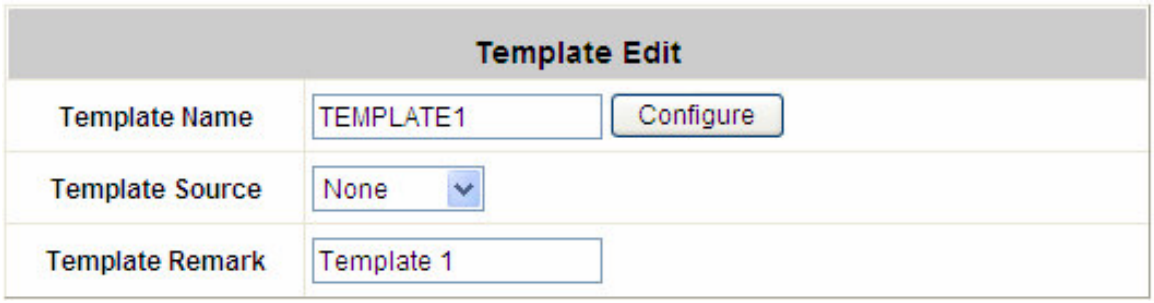
© 2008 4IPNET, INC.

4.3.4 Template Settings

Template is a model that can be copied to every AP and not necessary to configure the AP individually. There are three templates provided. Click ***Edit*** to go on configuration.



Before configure the template, copy the configuration mode of an AP to the template by selecting a **Source AP**, and without configuring the template from the beginning, administrators can also revise some settings for demand. If copy is not desired, please select **NONE**. Input the **Template Name** and **Template Remark** and click the button of ***Configure*** to go on configuration.



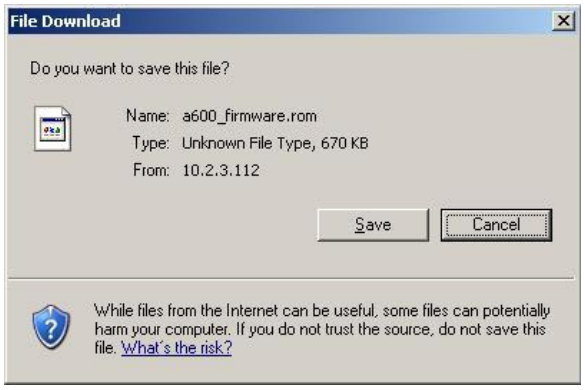
After entering the interface, revise the configuration for demand and change administrator's password if desired. About other function settings, please refer to **4.3.1 AP List**.

- **Template Editing**
  The administrator can set the template configuration manually. Click ***Configure*** button to have detailed configurations.

© 2008 4IPNET, INC.

4.3.5 Firmware Upload

Firmware Upload displays the current version of the AP's firmware. New firmware can be uploaded here to update the current firmware. To upload, click ***Browse*** to select the file and then click ***Upload***.


File Download
Do you want to save this file?
Name: a600_firmware.rom
Type: Unknown File Type, 670 KB
From: 10.2.3.112
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

© 2008 4IPNET, INC.

4.3.6 AP Upgrade

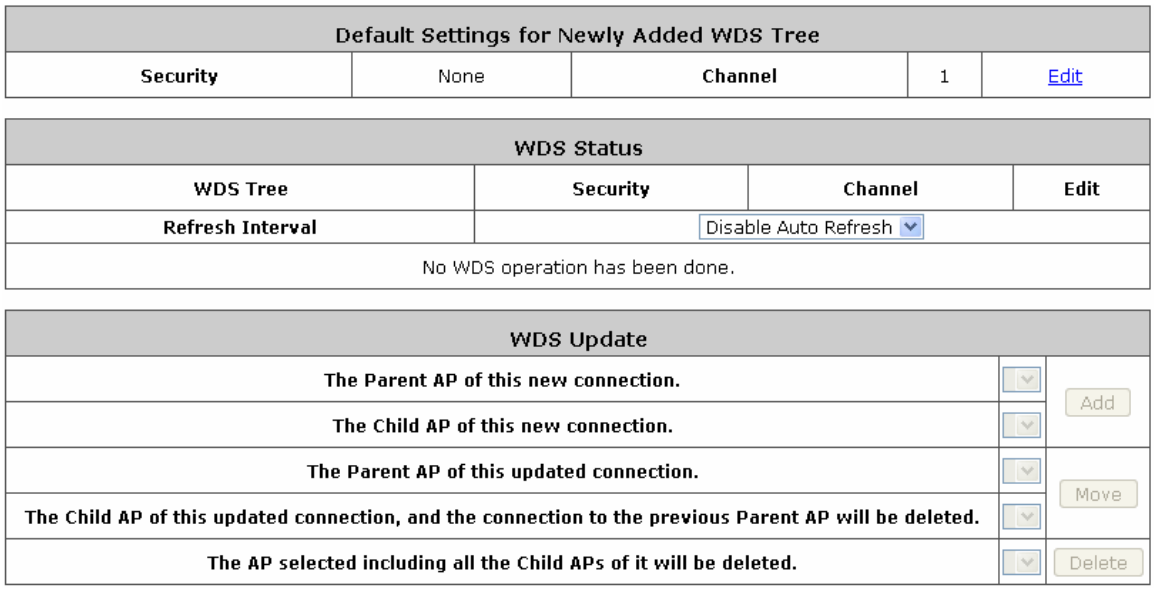
Check the APs which need to be upgraded and select the upgrade version of firmware, and click ***Apply*** to upgrade firmware.

AP List					
Name	Type	Version	Upgraded Time	New Version	Upgrade

© 2008 4IPNET, INC.

4.3.7 WDS Management

WDS Management (Wireless Distribution System) is a function used to connect **AP**s (Access Points) wirelessly. The WDS management function of the system can help administrators to setup a "Tree" structure of WDS network.

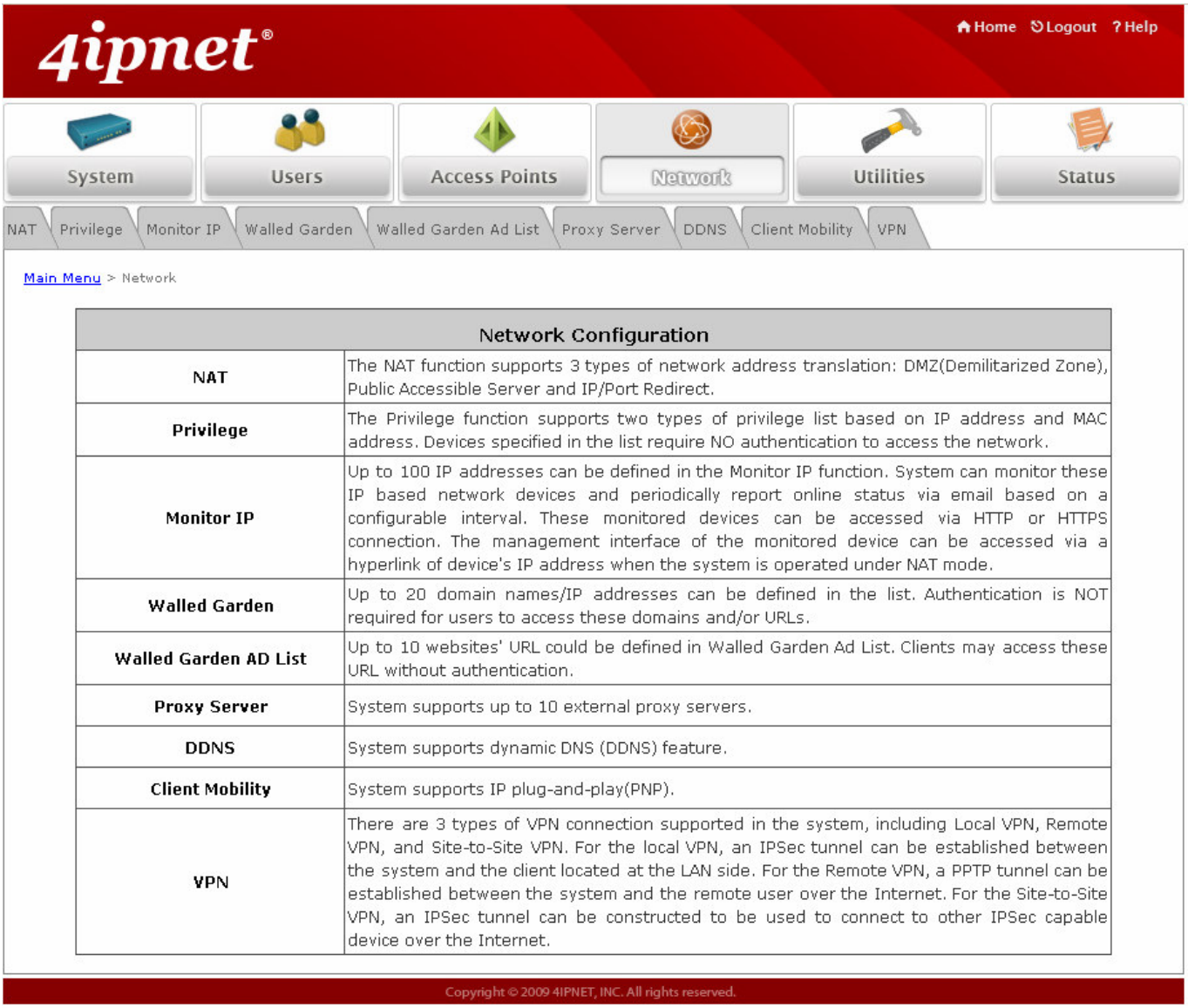


- **WDS Status:** Status shows the added APs in the WDS Tree with the Security and Channel settings. The WDS could be set up more than one tree. Click the ***Edit*** is to change the **WDS connection settings** for the associated WDS Tree.
- **WDS Update:** Update the WDS connection with the following operations.
  - ***Add*:** Add a new WDS connection with a Child AP not in the WDS and a Parent AP from the AP List. A new WDS Tree will be added if the selected Parent AP is not in any of the current WDS Trees. Click ***Edit*** is to change the **WDS connection settings** for the new added WDS Tree.
  - ***Move*:** Update a WDS connection with a Child AP from WDS and a Parent AP which could be anymore from WDS, and the previous WDS connection of the Child AP to the previous Parent AP will be deleted.
  - ***Delete*:** All the WDS connections of the selected AP will be deleted including the WDS connections to its Child APs, and the Child APs without wired connection will become unreachable.

© 2008 4IPNET, INC.

4.4 Network Configuration

This section includes the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Walled Garden AD List**, **Proxy Server Properties**, **Dynamic DNS**, **Client Mobility** and **VPN Configuration**.


4ipnet
Home
Logout
Help
System
Users
Access Points
Network
Utilities
Status
NAT
Privilege
Monitor IP
Walled Garden
Walled Garden Ad List
Proxy Server
DDNS
Client Mobility
VPN
Main Menu > Network
Network Configuration
NAT
The NAT function supports 3 types of network address translation: DMZ(Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege
The Privilege function supports two types of privilege list based on IP address and MAC address. Devices specified in the list require NO authentication to access the network.
Monitor IP
Up to 100 IP addresses can be defined in the Monitor IP function. System can monitor these IP based network devices and periodically report online status via email based on a configurable interval. These monitored devices can be accessed via HTTP or HTTPS connection. The management interface of the monitored device can be accessed via a hyperlink of device's IP address when the system is operated under NAT mode.
Walled Garden
Up to 20 domain names/IP addresses can be defined in the list. Authentication is NOT required for users to access these domains and/or URLs.
Walled Garden AD List
Up to 10 websites' URL could be defined in Walled Garden Ad List. Clients may access these URL without authentication.
Proxy Server
System supports up to 10 external proxy servers.
DDNS
System supports dynamic DNS (DDNS) feature.
Client Mobility
System supports IP plug-and-play(PNP).
VPN
There are 3 types of VPN connection supported in the system, including Local VPN, Remote VPN, and Site-to-Site VPN. For the local VPN, an IPSec tunnel can be established between the system and the client located at the LAN side. For the Remote VPN, a PPTP tunnel can be established between the system and the remote user over the Internet. For the Site-to-Site VPN, an IPSec tunnel can be constructed to be used to connect to other IPSec capable device over the Internet.
Copyright © 2009 4IPNET, INC. All rights reserved.

© 2008 4IPNET, INC.

4.4.1 Network Address Translation

Set the configuration for **DMZ, Public Accessible Server** and **Port and IP Redirect**.

Network Address Translation
DMZ (Demilitarized Zone)
Public Accessible Server
Port and IP Redirect

- **DMZ**

  The system supports up to 40 sets of Internal IP address (LAN) to External IP address (WAN) mapping in the Static Assignments. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN1) that will change dynamically if WAN1 Interface is Dynamic. When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with WAN1 interface. Each **Static Assignment** could be bound with the chosen External Interface, WAN1 or WAN2. There are 40 sets of static **Internal IP Address** and **External IP Address** available. Enter **Internal** and **External** IP Addresses as a set. After the setup, accessing the WAN will be mapped to access the Internal IP Address. These settings will become effective immediately after clicking the ***Apply*** button.

Automatic WAN IP Assignment

Enable	External IP Address	External Interface	Internal IP Address
☐	192.168.1.255	WAN1	

Static Assignments

No.	External IP Address	External Interface	Internal IP Address
1		WAN1	
2		WAN1	
3		WAN1	
4		WAN1	
5		WAN1	
6		WAN1	
7		WAN1	
8		WAN1	
9		WAN1	
10		WAN1	

(Total:40) First Prev Next Last

© 2008 4IPNET, INC.

- **Public Accessible Server**

  This function allows the administrator to set 40 virtual servers at most, so that client devices outside the managed network can access these servers within the managed network. Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general. Enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"**. Select **"TCP"** or **"UDP"** for the service's type. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the ***Apply*** button.

Public Accessible Server

Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				TCP UDP	
2				TCP UDP	
3				TCP UDP	
4				TCP UDP	
5				TCP UDP	
6				TCP UDP	
7				TCP UDP	
8				TCP UDP	
9				TCP UDP	
10				TCP UDP	

(Total:40) First Prev Next Last

- **Port and IP Redirect**

  This function allows the administrator to set 40 sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the **"IP Address"** and **"Port"** of **Destination**, and the **"IP Address"** and **"Port"** of **Translated to Destination**. Select **"TCP"** or **"UDP"** for the service's type.

© 2008 4IPNET, INC.

These settings will become effective immediately after clicking ***Apply***.

Port and IP Redirect					
No.	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					TCP UDP
2					TCP UDP
3					TCP UDP
4					TCP UDP
5					TCP UDP
6					TCP UDP
7					TCP UDP
8					TCP UDP
9					TCP UDP
10					TCP UDP

© 2008 4IPNET, INC.

4.4.2 Privilege List

Set the configuration for **Privilege IP Address List** and **Privilege MAC Address List**.

Privilege List
IP Address List
MAC Address List

- **Privilege IP Address List**

  If there are workstations inside the managed network that need to access the network without authentication, enter the IP addresses of these workstations in the **"Privilege IP Address List"**. The **"Remark"** field is not necessary but is useful to keep track. WHG303 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking ***Apply***.

Granted Access by IP Address		
No.	IP Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Permitting specific IP addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.

- **Privilege MAC Address List**

  In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in the **"Privilege MAC Address List"**. WHG303 allows 100 privilege MAC addresses at most. When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking ***Apply***.

© 2008 4IPNET, INC.

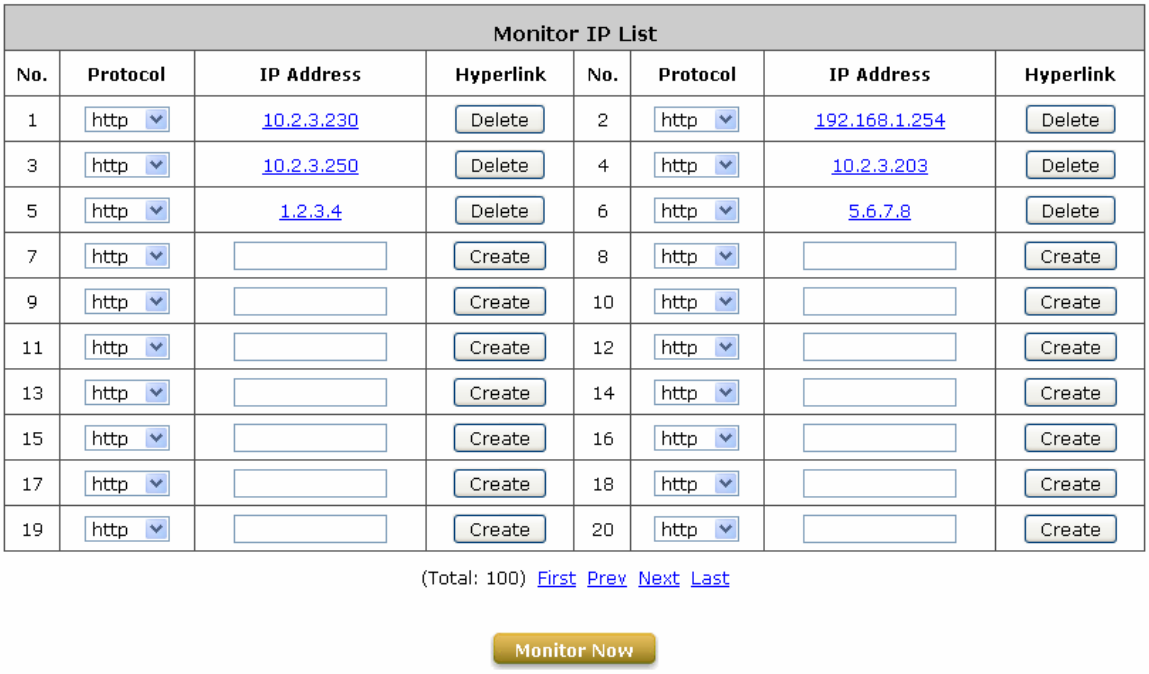
Granted Access by MAC Address		
No.	MAC Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Permitting specific MAC addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems

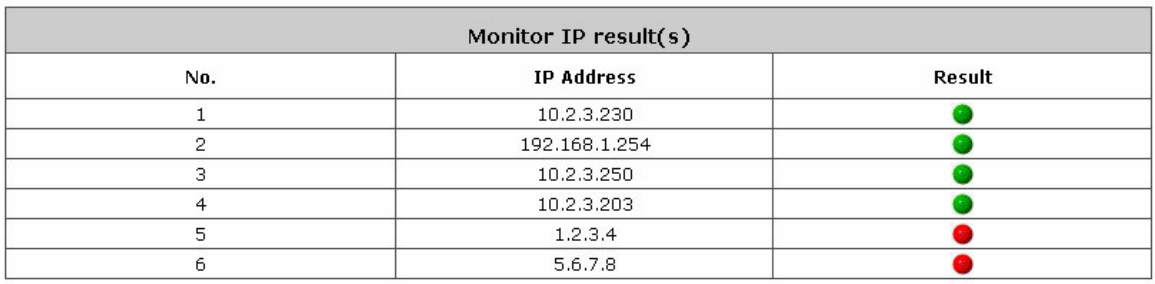
© 2008 4IPNET, INC.

4.4.3 Monitor IP List

WHG303 will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the necessary information, click ***Apply*** to save the settings. Click ***Monitor*** to check the current status of all the monitored IP. The system supports monitoring on 100 IP addresses listed in the **"Monitor IP List"**.


Monitor IP List
No. Protocol IP Address Hyperlink No. Protocol IP Address Hyperlink
1 http 10.2.3.230 Delete 2 http 192.168.1.254 Delete
3 http 10.2.3.250 Delete 4 http 10.2.3.203 Delete
5 http 1.2.3.4 Delete 6 http 5.6.7.8 Delete
7 http Create 8 http Create
9 http Create 10 http Create
11 http Create 12 http Create
13 http Create 14 http Create
15 http Create 16 http Create
17 http Create 18 http Create
19 http Create 20 http Create
(Total: 100) First Prev Next Last
Monitor Now

On each monitored item with a WEB server running, administrators may add a link for the easy access by selecting a protocol, http or https, and click the ***Add*** button. After clicking ***Add*** button, the IP address will become a hyperlink, and administrators can easily access the host by clicking the hyperlink remotely. Click the ***Del*** button to remove the setting.



© 2008 4IPNET, INC.

4.4.4 Walled Garden List

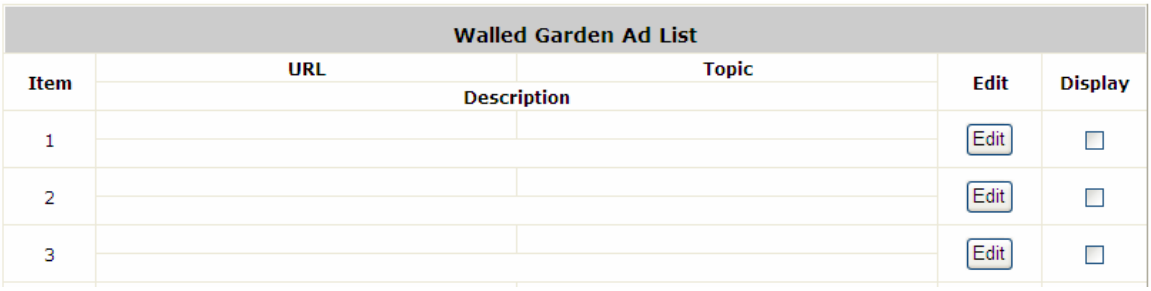
This function provides certain free services for users to access the websites listed here before login and authentication. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website **IP Address** or **Domain Name** in the list and click ***Apply*** to save the settings.

Walled Garden List			
No.	**Domain Name/IP Address**	**No.**	**Domain Name/IP Address**
1	www.google.com	2	www.yahoo.com
3	www.your_website.com	4	www.your_ad.com
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

© 2008 4IPNET, INC.

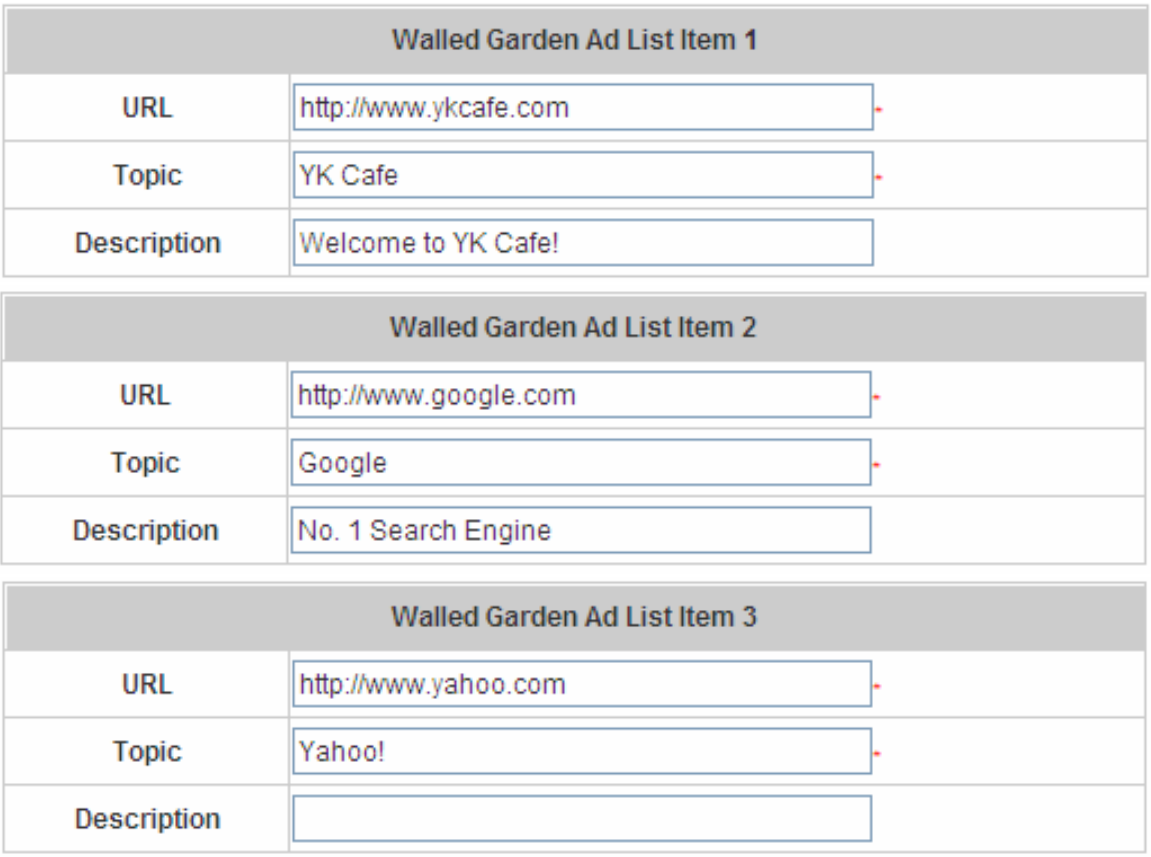
4.4.5 Walled Garden Ad List

This function provides advertisement web pages for users to access free advertisement websites listed before login and authentication. Advertisement hyperlinks are displayed on the user's login page. Clients who click on it will be redirected to the listed advertisement websites.



Walled Garden Ad List				
Item	URL Description	Topic	Edit	Display
1			Edit	☐
2			Edit	☐
3			Edit	☐

- **Edit:** Click ***Edit*** to add a new item or make changes. Click ***Apply***, the items will be added and shown in the list.
- **Display:** Choose ***Display*** to display advertisement hyperlinks on the login pages



Walled Garden Ad List Item 1	
URL	http://www.ykcafe.com
Topic	YK Cafe
Description	Welcome to YK Cafe!

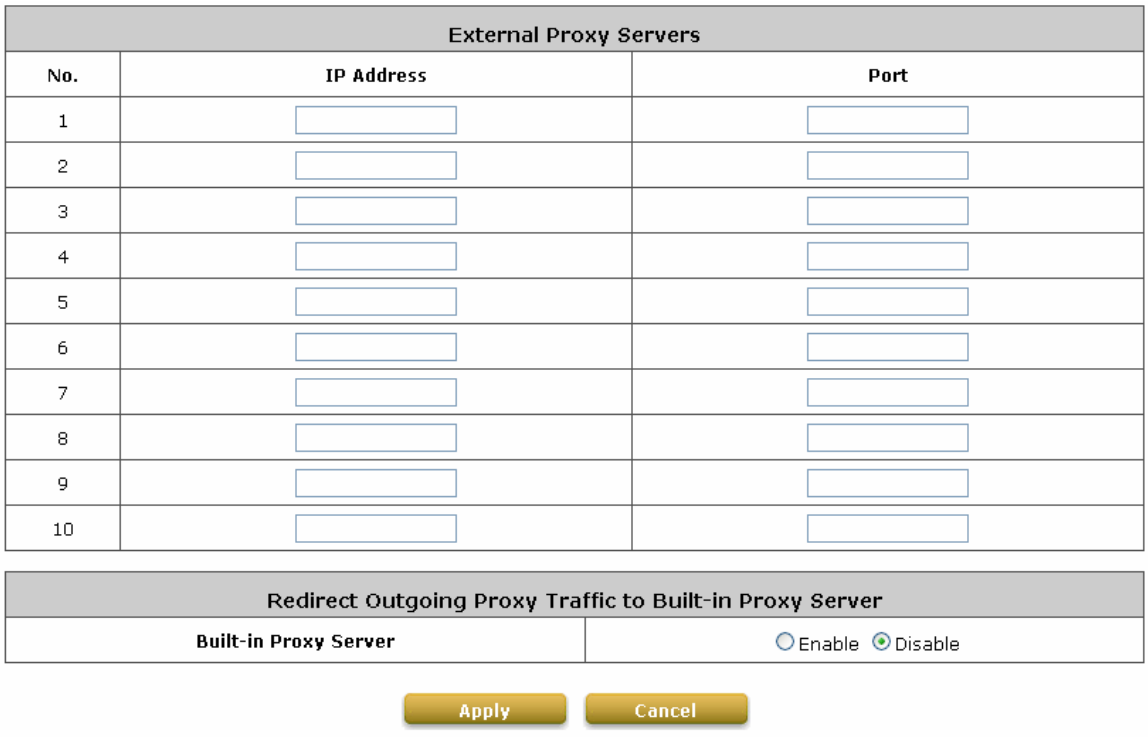
Walled Garden Ad List Item 2	
URL	http://www.google.com
Topic	Google
Description	No. 1 Search Engine

Walled Garden Ad List Item 3	
URL	http://www.yahoo.com
Topic	Yahoo!
Description	

© 2008 4IPNET, INC.

4.4.6 Proxy Server Properties

WHG303 supports Internal Proxy Server and External Proxy Server functions.



- **External Proxy Server:** Under the security management of WHG303, the system will match the External Proxy Server list to the clients' proxy settings. If there is not a match, the clients will not be able to reach the login page and thus unable to access the network. If there is a match, the clients will be directed to the system for authentication. After a successful authentication, the clients will be redirected back to the desired proxy servers depending on different situations.

- **Internal Proxy Server:** WHG303 has a built-in proxy server. If this function is enabled, the clients will be forced to treat WHG303 as the proxy server regardless of their original proxy settings.

  For more details about how to set up the proxy servers, please refer to **Appendix E. Proxy Setting.**

© 2008 4IPNET, INC.

4.4.7 Dynamic DNS

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider. WHG303 supports DNS function to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access WHG303's WAN. If the dynamic DHCP is activated at the WAN port, it will update the IP address of the DNS server periodically. These settings will become effective immediately after clicking ***Apply***.

Dynamic DNS	
DDNS	○ Enable ◉ Disable
Provider	DynDNS.org(Dynamic)
Host Name	*
Username/E-mail	admin *
Password/Key	••••• *

- **DDNS:** Enable or disable this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

Note: To apply for free Dynamic DNS service, you may go to http://www.dyndns.com/services/dns/dyndns/howto.html.

© 2008 4IPNET, INC.

4.4.8 Client Mobility

WHG303 supports IP PNP function.

Client Mobility	
IP PNP	○ Enable ◉ Disable

At the user end, a static IP address can be used to connect to the system. Regardless of what the IP address at the user end is, authentication can still be performed through WHG303.

© 2008 4IPNET, INC.

4.4.9 VPN Configuration

***V**irtual **P**rivate **N**etwork*, or **VPN**, a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

VPN Settings
Local VPN
Remote VPN
Site-to-Site VPN

Local VPN: Local VPN allows to create the VPN tunnel between a user's device and WHG303, to encrypt the data transmission. In addition, only when this function is enabled (***Active***) here do users of the entire system are able to use Local VPN. Local VPN users can also be isolated from each other when ***VPN Client Isolation*** is enabled.

Local VPN For The Entire System	
Active	◉ Enable ○ Disable
VPN Client Isolation	○ Enable ◉ Disable

IPSec Parameters	
Encryption	○ DES ◉ 3-DES
Integrity	◉ MD5 ○ SHA-1
Diffie-Hellman	◉ Group 1 ○ Group 2

For more information about Local VPN, please see ***Appendix I. Local VPN***.

Remote VPN: When the setting is enabled, the system allows the VPN tunnel between a remote client and the system to encrypt the data transmission via PPTP. The system's VPN supports end-users' device under Windows 2000, Windows XP SP1, SP2 and Windows Vista. Start IP field must be entered when enabled. The supported Authentication Servers, Group Permission, Client Policy, and the Remote VPN login page also can be configured here. The system supports up to 10 PPTP connections.

© 2008 4IPNET, INC.

Remote VPN for the Entire System					
Remote VPN Status	○ Enable ◉ Disable				
IP Address Range Assignment	Start IP Address: 192.168.6.1 *(Support up to 10 connections.)				
SIP Configuration	Enable ☐ WAN Interface WAN1				
Authentication Options	**Auth Option**	**Auth Database**	**Postfix**	**Default**	**Enabled**
	Server 1	LOCAL	local	◉	☑
	Server 2	POP3	pop3	○	☑
	Server 3	RADIUS	radius	○	☑
	Server 4	LDAP	ldap	○	☑
Group Permission Configuration	Configure				
Applied Policy to Remote Client	Policy 1				
Remote VPN Login Page	Configure				

Site-to-site VPN: When the setting is enabled, the system enables the IPSec VPN tunnel to reach remote networks/sites with encrypted data transmission. Click ***Add A Remote Site*** button to set configuration about remote VPN capable devices such as VPN gateway. Click ***Add A Local Site*** button to set configuration about local site.

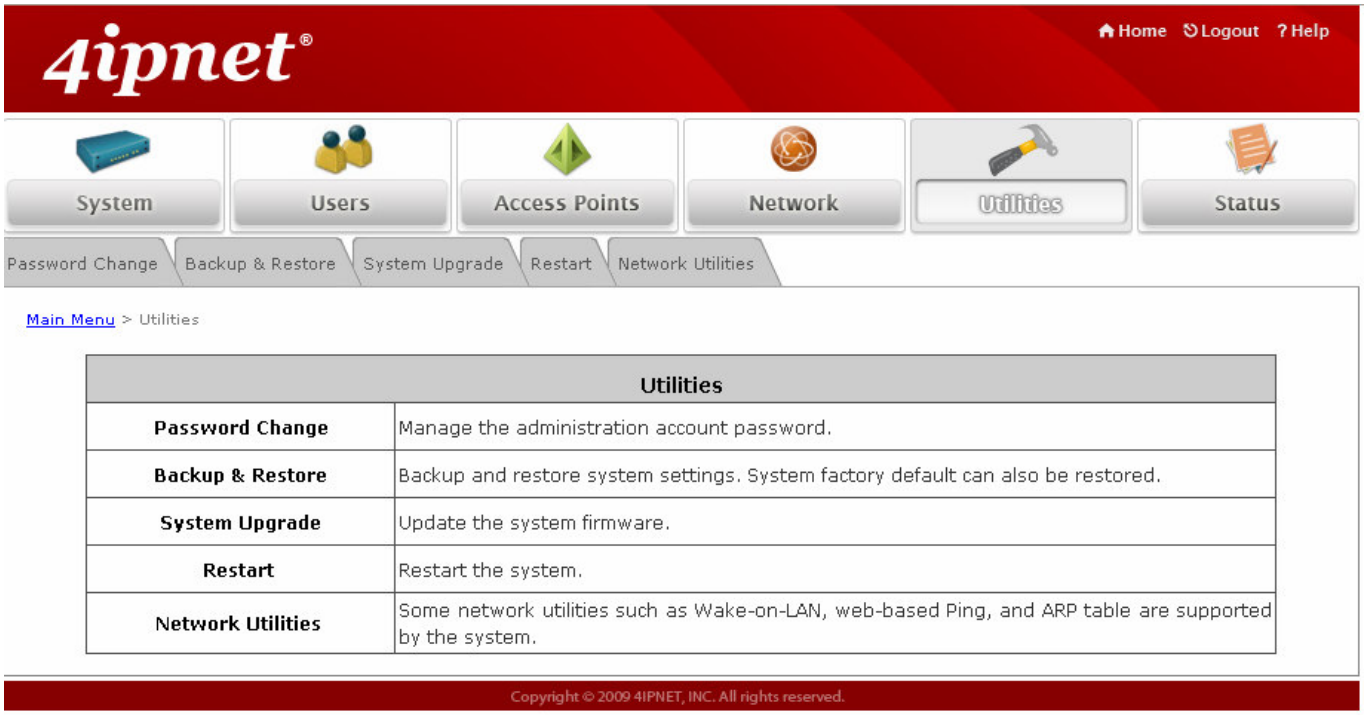
Remote Site Configuration				
Name	**IP Address**	**Pre-shared Key**	**Edit**	**Delete**
Add A Remote Site				

Local Site Configuration					
Local Subnet	**Local Interface**	**Remote VPN Gateway**	**Remote Subnet**	**Edit**	**Delete**
Add A Local Site					

© 2008 4IPNET, INC.

4.5 Utilities

This section provides utilities to customize and maintain the system including **Change Password**, **Backup&Restore Settings**, **System Upgrade, Restart** and **Network Utilities**.



© 2008 4IPNET, INC.

4.5.1 Change Password

There are three levels of authorities: **admin**, **manager** or **operator**. The default usernames and passwords are as follows:

Admin: The administrator can access all configuration pages of WHG303.

User Name: **admin**

Password: **admin**

Manager: The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts, but without permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

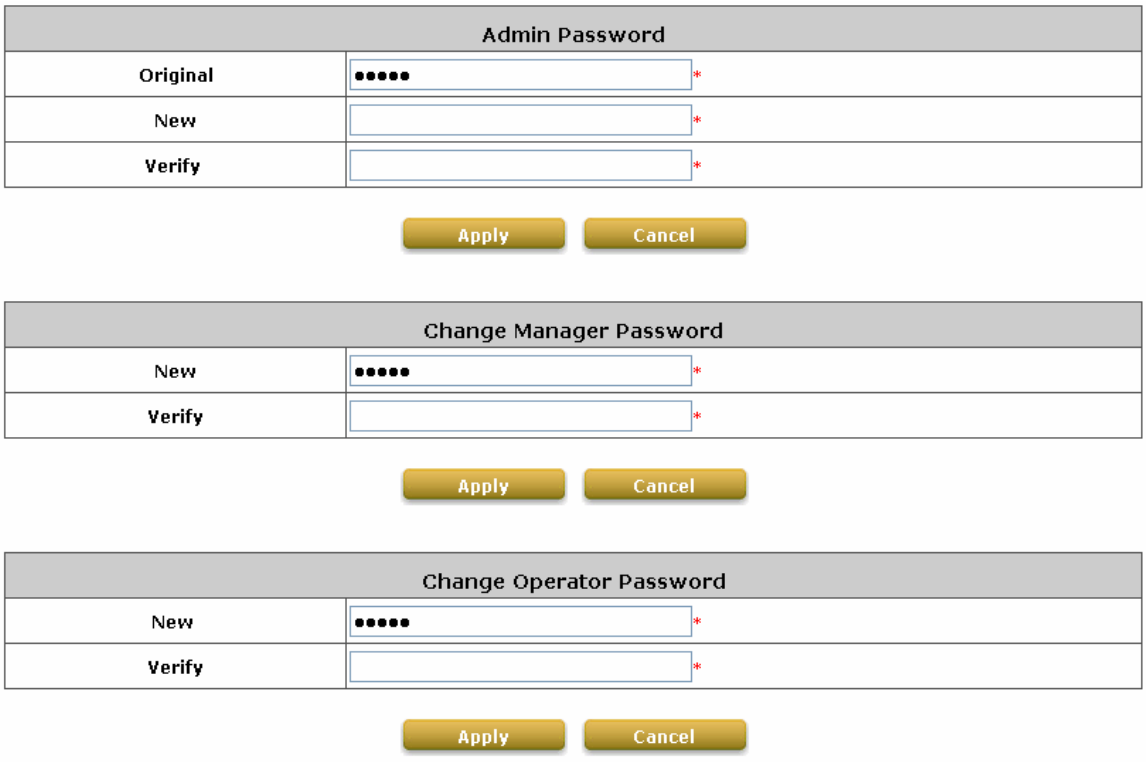
Password: **manager**

Operator: The operator can only access the configuration page of ***Create On-demand User*** to create new on-demand user accounts and print out the on-demand user account receipts.

User Name: **operator**

Password: **operator**

The administrator can change the passwords here. Please enter the current password and then enter the new password twice to verify. Click ***Apply*** to activate this new password.



© 2008 4IPNET, INC.

If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface at the serial console port.

4ipnet WHG303 supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default usernames and passwords show as follows:

Admin: The administrator can access all configuration pages of WHG303.

User Name: **admin**

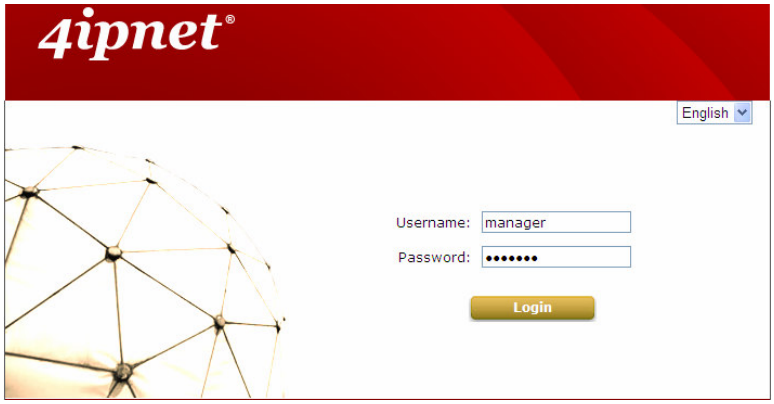
Password: **admin**

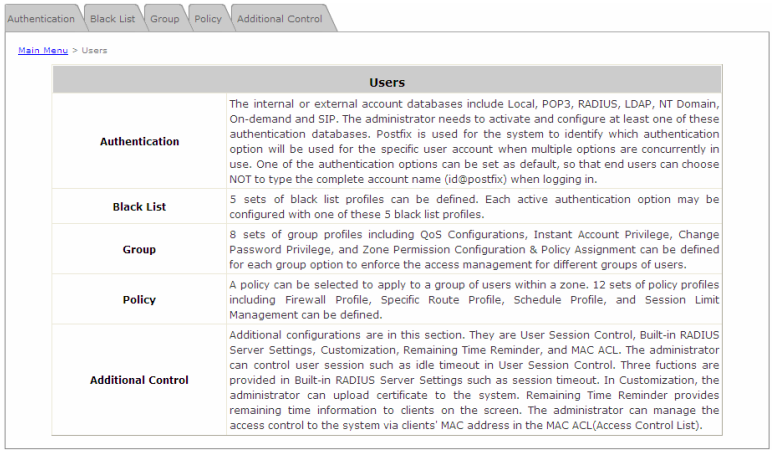
Manager: The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts, but without the permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **manager**

© 2008 4IPNET, INC.



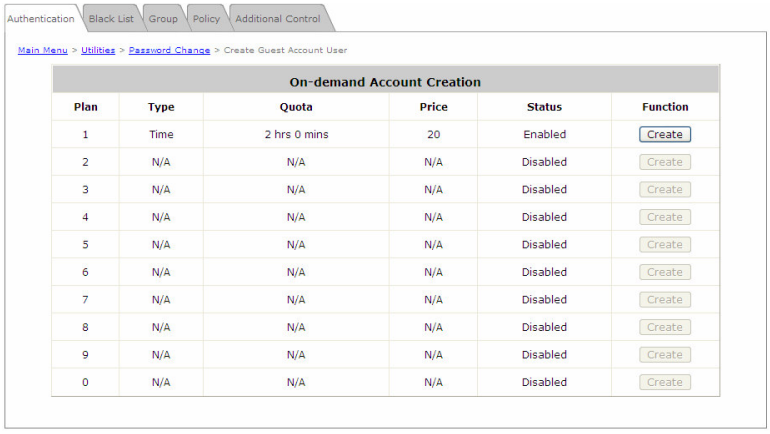

Authentication
Black List
Group
Policy
Additional Control
Main Menu > Users
Users
Authentication
The internal or external account databases include Local, POP3, RADIUS, LDAP, NT Domain, On-demand and SIP. The administrator needs to activate and configure at least one of these authentication databases. Postfix is used for the system to identify which authentication option will be used for the specific user account when multiple options are concurrently in use. One of the authentication options can be set as default, so that end users can choose NOT to type the complete account name (id@postfix) when logging in.
Black List
5 sets of black list profiles can be defined. Each active authentication option may be configured with one of these 5 black list profiles.
Group
8 sets of group profiles including QoS Configurations, Instant Account Privilege, Change Password Privilege, and Zone Permission Configuration & Policy Assignment can be defined for each group option to enforce the access management for different groups of users.
Policy
A policy can be selected to apply to a group of users within a zone. 12 sets of policy profiles including Firewall Profile, Specific Route Profile, Schedule Profile, and Session Limit Management can be defined.
Additional Control
Additional configurations are in this section. They are User Session Control, Built-in RADIUS Server Settings, Customization, Remaining Time Reminder, and MAC ACL. The administrator can control user session such as idle timeout in User Session Control. Three fuctions are provided in Built-in RADIUS Server Settings such as session timeout. In Customization, the administrator can upload certificate to the system. Remaining Time Reminder provides remaining time information to clients on the screen. The administrator can manage the access control to the system via clients' MAC address in the MAC ACL(Access Control List).

Operator: The operator can only access the configuration page of ***Create On-demand User*** to create new on-demand user accounts and print out the on-demand user account receipts.

User Name: **operator**

Password: **operator**

© 2008 4IPNET, INC.

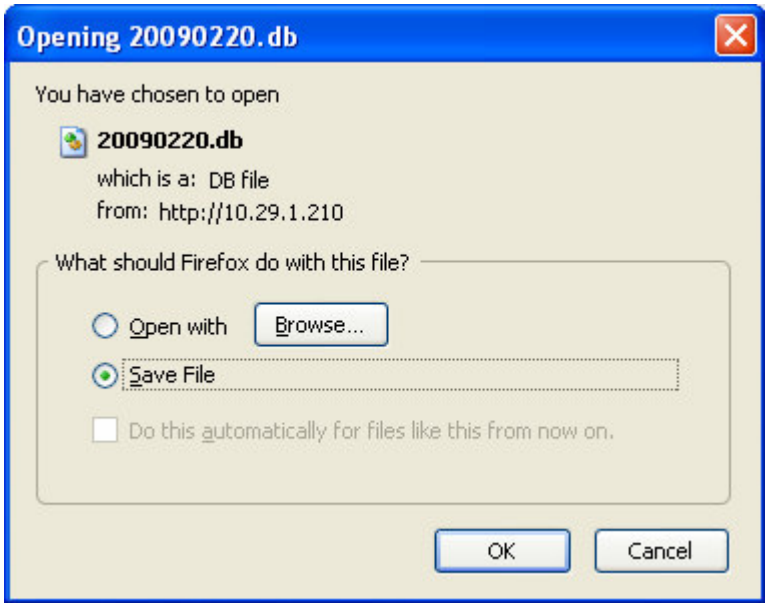

Authentication
Black List
Group
Policy
Additional Control
Main Menu > Utilities > Password Change > Create Guest Account User
On-demand Account Creation
Plan
Type
Quota
Price
Status
Function
1 Time 2 hrs 0 mins 20 Enabled Create
2 N/A N/A N/A Disabled Create
3 N/A N/A N/A Disabled Create
4 N/A N/A N/A Disabled Create
5 N/A N/A N/A Disabled Create
6 N/A N/A N/A Disabled Create
7 N/A N/A N/A Disabled Create
8 N/A N/A N/A Disabled Create
9 N/A N/A N/A Disabled Create
0 N/A N/A N/A Disabled Create

© 2008 4IPNET, INC.

4.5.2 Backup/Restore Settings

This function is used to backup/restore the 4ipnet WHG303 settings. Also, WHG303 can be restored to the factory default settings here.

- **Backup current system settings:** Click ***Backup*** to create a .db database backup file and save it on disk.



- **Restore system settings:** Click ***Browse*** to search for a .db database backup file created by WHG303 and click ***Restore*** to restore to the same settings at the time when the backup file was saved.
- **Reset to the factory-default settings:** Click ***Reset*** to load the factory default settings of WHG303.

© 2008 4IPNET, INC.

4.5.3 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click ***Browse*** to search for the firmware file and click ***Apply*** for the firmware upgrade. It might take a few minutes before the upgrade process completes and the system needs to be restarted afterwards to activate the new firmware.

1. *Firmware upgrade may cause the loss of some data. Please refer to the release notes for the limitation before upgrading.*
2. *Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or restart process. It may damage the system and cause malfunction.*

© 2008 4IPNET, INC.

4.5.4 Restart

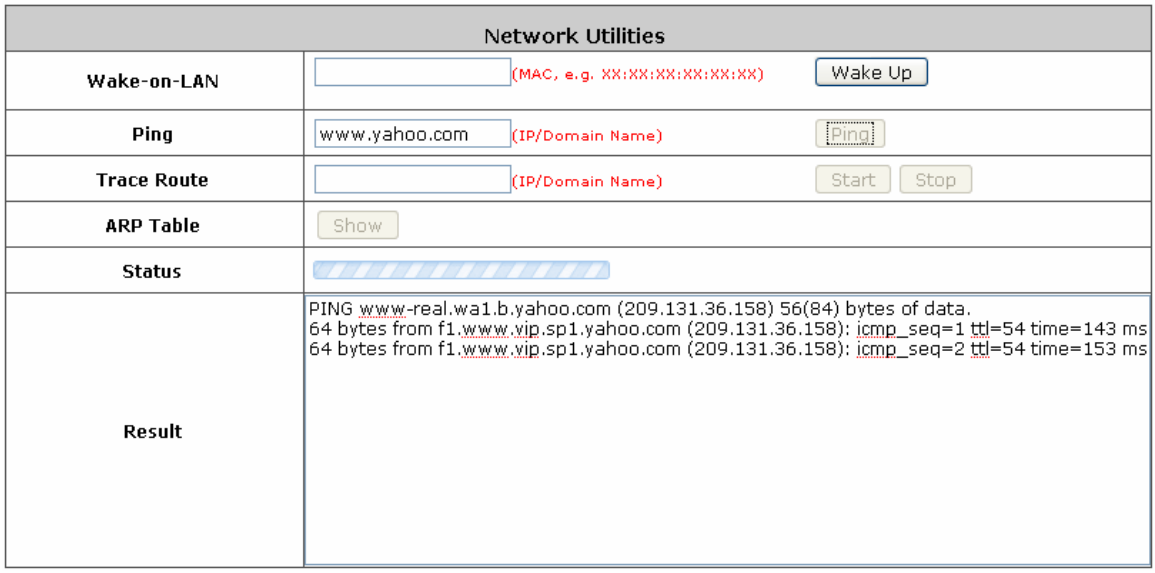
This function allows the administrator to safely restart 4ipnet WHG303, and the process might take approximately three minutes. Click ***YES*** to restart WHG303; click ***NO*** to go back to the previous screen. If the power needs to be turned off, it is highly recommended to restart WHG303 first and then turn off the power after completing the restart process.

The connection of all online users of the system will be disconnected when system is in the process of restarting.

© 2008 4IPNET, INC.

4.5.5 Network Utilities

This function allows the administrators to manage functions including **Wake-on-LAN**, **Ping**, **Trace Route**, and showing **ARP Table** by entering IP or Domain Name.

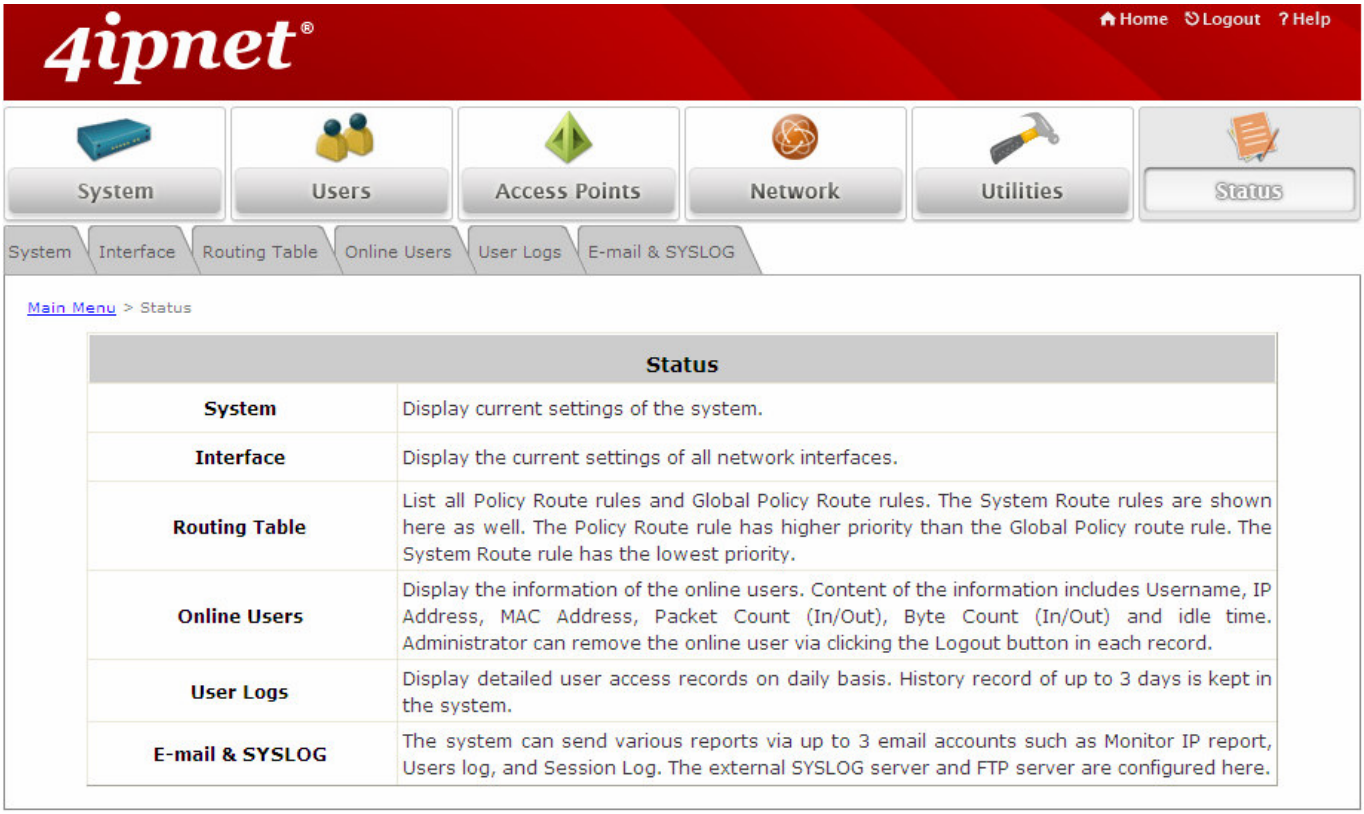


- **Wake on LAN:** It allows the system to remotely boot up a power-down computer with Wake-On-LAN feature enabled and is on the LAN side. Enter the MAC Address of the desired device and click Wake Up button to execute this function.
- **Ping:** It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.
- **Trace Route:** It allows administrator to find out the real path of packets from the gateway to a destination using IP address or Host domain name.
- **ARP Table:** It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).

© 2008 4IPNET, INC.

4.6 Status

This section includes **System Status**, **Interface Status**, **Routing Table**, **Online Users**, **User Logs**, and **E-mail & SYSLOG** to provide system status information and online user status.



Status	
System	Display current settings of the system.
Interface	Display the current settings of all network interfaces.
Routing Table	List all Policy Route rules and Global Policy Route rules. The System Route rules are shown here as well. The Policy Route rule has higher priority than the Global Policy route rule. The System Route rule has the lowest priority.
Online Users	Display the information of the online users. Content of the information includes Username, IP Address, MAC Address, Packet Count (In/Out), Byte Count (In/Out) and idle time. Administrator can remove the online user via clicking the Logout button in each record.
User Logs	Display detailed user access records on daily basis. History record of up to 3 days is kept in the system.
E-mail & SYSLOG	The system can send various reports via up to 3 email accounts such as Monitor IP report, Users log, and Session Log. The external SYSLOG server and FTP server are configured here.

© 2008 4IPNET, INC.

4.6.1 System Status

This section provides an overview of the system for the administrator.

System Setting Overview		
Firmware Version		1.00.00-EN-N
Build		00200
System Name		Wireless Hotspot Gateway
Homepage Redirect URL		http://www.google.com
SYSLOG Server - System Log		N/A:N/A
SYSLOG Server - On-demand Users Log		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
User Logs	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
System Time	NTP Server	tock.usno.navy.mil
	Time	2009/02/19 16:59:50 +0800
User Session Control	Idle Time Out	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

© 2008 4IPNET, INC.

The description of the above-mentioned table is as follows:

Item		***Description***
Current Firmware Version		The present firmware version of WHG303
Build		The current build number.
System Name		The system name. The default is WHG303
Home Page		The page the users are directed to after initial login success.
Syslog server-Traffic History		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Syslog server-On demand User log		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Proxy Server		Enabled/disabled stands for that the system is currently using the proxy server or not.
Warning of Internet Disconnection		Enabled/Disabled stands for the connection at WAN is normal or abnormal (**Internet Connection Detection**) and all online users are allowed/disallowed to log in the network.
WAN Failover		Enabled/Disabled stands for the function currently being used or not.
Load Balancing		Enabled/Disabled stands for the function currently being used or not.
SNMP		Enabled/disabled stands for the current status of the SNMP management function.
History	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Email To	The email address to which the traffic history or user's traffic history information will be sent.
Time	**NTP Server**	The network time server that the system is set to align.
	Date Time	The system time is shown as the local time.
User	**Idle Timer**	The minutes allowed for the users to be inactive before their account expires automatically.
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

© 2008 4IPNET, INC.

4.6.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **SZ Default~8**.

Network Interface		
WAN1	**MAC Address**	00:16:E6:81:C4:A8
	IP Address	192.168.1.254
	Subnet Mask	255.255.0.0
WAN2	**Disabled**	
	WAN1	**WAN2**
Packets In	152715 (Δ 5986)	0 (Δ 0)
Packets Out	4291 (Δ 3862)	0 (Δ 0)
Bytes In	16708157 (Δ 887788)	0 (Δ 0)
Bytes Out	3272816 (Δ 3240801)	0 (Δ 0)
Service Zone - Default	**Mode**	NAT
	MAC Address	00:16:E6:81:C4:A9
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
Service Zone - Default DHCP Server	**Status**	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
Service Zone - SZ1	**Disabled**	

-
-
-

Service Zone - SZ8	**Disabled**

© 2008 4IPNET, INC.

The description of the above-mentioned table is as follows:

Item		***Description***
WAN1	**MAC Address**	The MAC address of the WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
WAN2	**MAC Address**	The MAC address of the WAN2 port.
	IP Address	The IP address of the WAN2 port.
	Subnet Mask	The Subnet Mask of the WAN2 port.
Packets In		The total accumulated packets in through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Packets Out		The total accumulated packets out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Bytes In		The total accumulated bytes in through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Bytes Out		The total accumulated packets out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Service Zone - Default DHCP Server	**Status**	Enable/disable stands for status of the DHCP server in Default Service Zone
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
Service Zone – Default	**Mode**	The operation mode of the default SZ.
	MAC Address	The MAC address of the default SZ.
	IP Address	The IP address of the default SZ.
	Subnet Mask	The Subnet Mask of the default SZ.

© 2008 4IPNET, INC.

4.6.3 Routing Table

All the **Policy** Route rules and **Global Policy** Route rules will be listed here. Also it will show the **System** Route rules specified by each interface.

Policy 1			
Destination	Subnet Mask	Gateway	Interface

Policy 2			
Destination	Subnet Mask	Gateway	Interface

Policy 3			
Destination	Subnet Mask	Gateway	Interface

Policy 4			
Destination	Subnet Mask	Gateway	Interface

•
•
•

Policy 12			
Destination	Subnet Mask	Gateway	Interface

Global Policy			
Destination	Subnet Mask	Gateway	Interface

System			
Destination	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	Default
	255.255.0.0	0.0.0.0	WAN1
0.0.0.0	0.0.0.0		WAN1

© 2008 4IPNET, INC.

- **Policy 1~12:** Shows the information of the individual Policy from 1 to 12.
- **Global Policy:** Shows the information of the Global Policy.
- **System:** Shows the information of the system administration.
  - **Destination:** The destination IP address of the device.
  - **Subnet Mask:** The Subnet Mask IP address of the port.
  - **Gateway**: The Gateway IP address of the port.
  - **Interface:** The choice of interface network, including **WAN1**, **WAN2**, **Default**, or the named **Service Zones** to be applied for the traffic interface.

© 2008 4IPNET, INC.

4.6.4 Online Users List

In this function, each online user's information including **Username**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle**, **Access From** and **Kick Out** will be shown. Administrators can force out a specific online user by clicking the hyperlink of ***"Logout"*** and check the user access AP status by clicking the hyperlink of the AP name for "**Location**." Click ***Refresh*** is to update the current users list.

© 2008 4IPNET, INC.

4.6.5 Users Logs

This function is used to check the traffic history of 4ipnet WHG303. The history of each day will be saved separately in the DRAM for at least 3 days (72 full hours). The system also keeps a cumulated record of the traffic data generated by each user in the latest 2 calendar months.

Users Log	
Date	**Size (Byte)**
2009-02-18	65
2009-02-19	65
2009-02-20	65
On-demand Users Log	
Date	**Size (Byte)**
2009-02-18	105
2009-02-19	105
2009-02-20	105
Roaming Out User Log	
Date	**Size (Byte)**
2009-02-18	106
2009-02-19	106
2009-02-20	106
Roaming In User Log	
Date	**Size (Byte)**
2009-02-18	112
2009-02-19	112
2009-02-20	112
SIP Call Usage Log	
Date	**Call Count**
2009-02-18	0
2009-02-19	0
2009-02-20	0

Monthly Network Usage of Local User		
Month	**No. of Entries**	**Usage Data**
2009-02	3	Download

Since the history is saved in the DRAM, if you need to restart the system, and at the same time, keep the history, please manually copy and save the traffic history information before restarting.

If the **History Email** has been entered under the **Notify Configuration** page, the system will automatically send out the history information to that specified email address.

- **Traffic History**

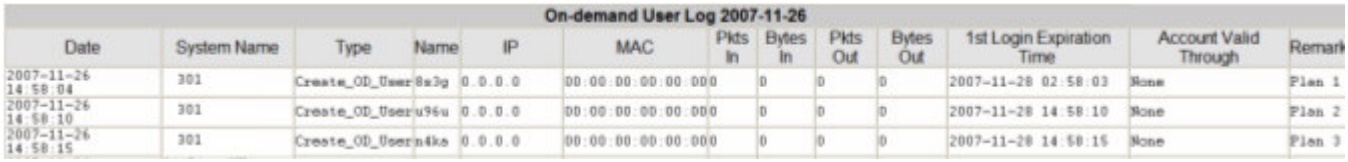
  All activities occur on the system within the nearest 72 hours are recorded; in date and time order. As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type, Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out** and **Bytes Out** of the user activities.

Users Log 2009-02-18								
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out

© 2008 4IPNET, INC.

- **On-demand User Log**

  As shown in the following figure, each line is a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, 1st Login Expiration Time**, **Account Valid Through** and **Remark**, of user activities.



On-demand User Log 2007-11-26

Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	1st Login Expiration Time	Account Valid Through	Remark
2007-11-26 14:58:04	301	Create_OD_User	8s3g	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:03	None	Plan 1
2007-11-26 14:58:10	301	Create_OD_User	u96u	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:10	None	Plan 2
2007-11-26 14:58:15	301	Create_OD_User	n4ks	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:15	None	Plan 3

- **Roaming Out Traffic History**

  As shown in the following figure, each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming Out User Log 2009-02-18

Date	Type	Name	NASID	NASIP	NASPort	UserMAC	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **Roaming In Traffic History**

  As shown in the following figure, each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming In User Log 2009-02-18

Date	Type	Name	NASID	NASIP	NASPort	UserMAC	UserIP	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **SIP Call Usage Log**

  The log provides the login and logout activities of SIP clients (device and soft clients) such as Start Time, Caller, Callee and Duration (seconds)

SIP Call Usage Log

Start Time	Caller	Callee	Duration (seconds)

© 2008 4IPNET, INC.

- **Monthly Network Usage of Local User**

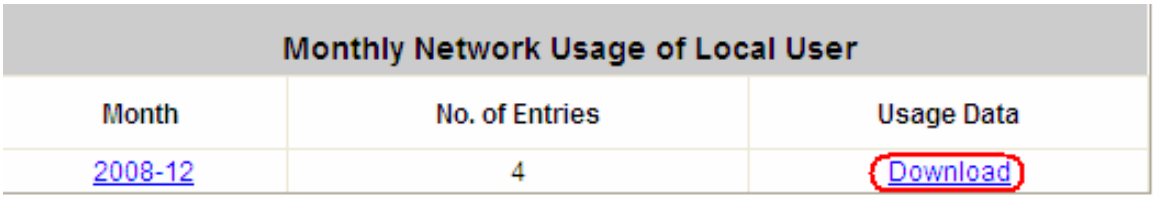
  The system keeps a cumulated record of the traffic data generated by each user in the latest 2 calendar months. As shown in the following figure, each line in a monthly network usage of local user record consists of 6 fields, **Username**, **Connection Time Usage**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out** of user activities.

Monthly Report 2009-02					
Username	Connection Time Usage	Packets In	Bytes In	Packets Out	Bytes Out
test	0	0	0	0	0
user1	0	0	0	0	0
user2	0	0	0	0	0

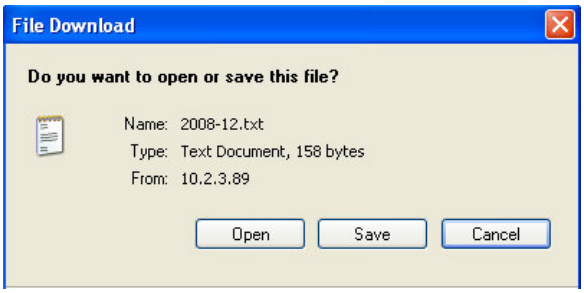
(Total: 3)
First Prev Next Last

  - **Username:** Username of the local user account.
  - **Connection Time Usage:** The total time used by the user.
  - **Pkts In/ Pkts Out:** The total number of packets received and sent by the user.
  - **Bytes In/ Bytes Out:** The total number of bytes received and sent by the user.

➢ **Download Monthly Network Usage of Local User:** Click on the ***Download*** button for outputting the report manually to a local database.



A warning message will then appear. Click ***Save*** to download the record into .txt format.

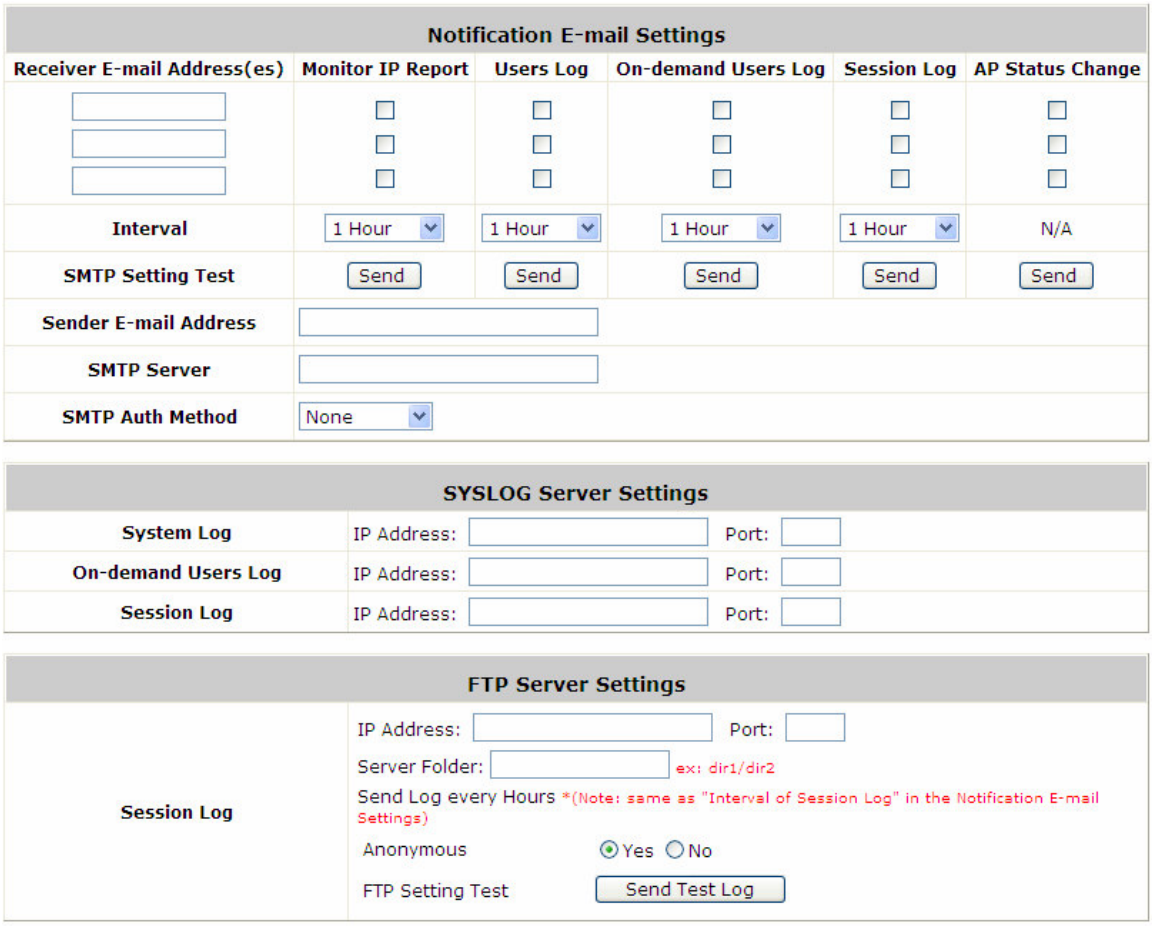



```
Username,Connection Time Usage,Packets In,Bytes In,Packets Out,Bytes Out
1,12,62,4588,64,6061
laurel,153,397,346078,337,36728
tom,0,0,0,0,0
u1,0,0,0,0,0
```


© 2008 4IPNET, INC.

4.6.6 E-mail & SYSLOG

WHG303 can automatically send the notification of **Monitor IP Report**, **Traffic History**, **On-demand User Log**, **Session Log** and **AP status** to up to 3 particular e-mail address. The notification of AP Status is triggered by the event when a managed AP becomes unreachable while the other types of emails are sent periodically in given intervals such as 1 hour. A trial email is provided by the system for validation. In addition, the system supports recording Syslog of Traffic History, On-demand User Log and Session Log via external Syslog servers. In addition, the Session Log can be sent to a specified FTP server. Enter the related information and select the desired items and then apply the settings.



© 2008 4IPNET, INC.

- **E-mail Notification Configuration:**
  - **Send To:** Up to 3 e-mail address can be set up to receive the notification. These are the receiver's e-mail addresses. There are four kinds of notification to selection -- Monitor IP Report, Traffic History, On-demand User Log and AP Status, and check which type of notification to be sent.
  - **Interval:** The time interval to send the e-mail report.
  - **Send Test Email:** To test the settings immediately.
  - **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
  - **SMTP:** The IP address of the sender's SMTP server.
  - **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.
    - **NTLMv1** is not currently available for general use.
    - **Plain** and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express use **Login** as default, although they can be set to use **NTLMv1**.
    - Pegasus uses **CRAM-MD5** or **Login** but which method to be used can not be configured.

- **Syslog Configuration:** There are 3 types of Syslog supported: System Log, On-demand User Log, and Session Log. Enter the IP address and Port number to specify which and from where the report should be sent to.

Note: When the number of a user's session (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this Syslog server.

- **FTP Server Settings**

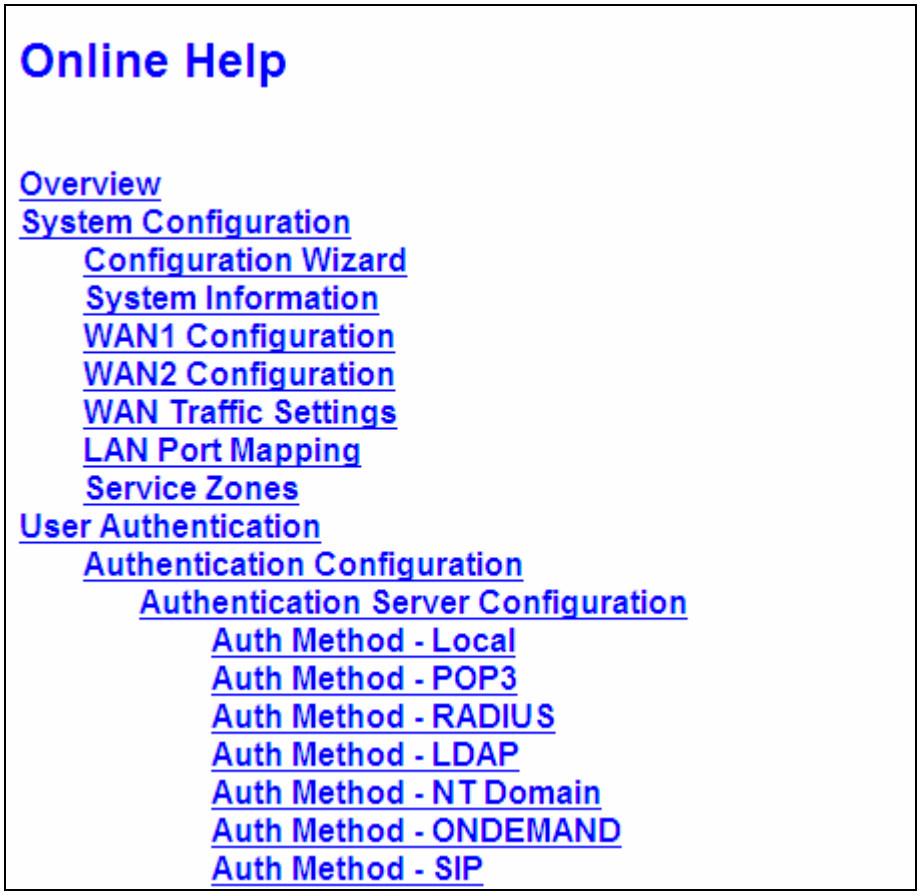
Session Log: Log each connection created by users and tracking the source IP and destination IP. If Syslog is enabled, Session Log will be sent to the Syslog server automatically during every defined interval in Session Log email notification. Session Log allows uploading the log file to a FTP server periodically. The maximum log file size is 256K. The log file will be sent to the FTP server once the file size reaches its maximum size or periodical time interval.

© 2008 4IPNET, INC.

4.7 Help

On the screen, the **Help** button is on the upper right corner.

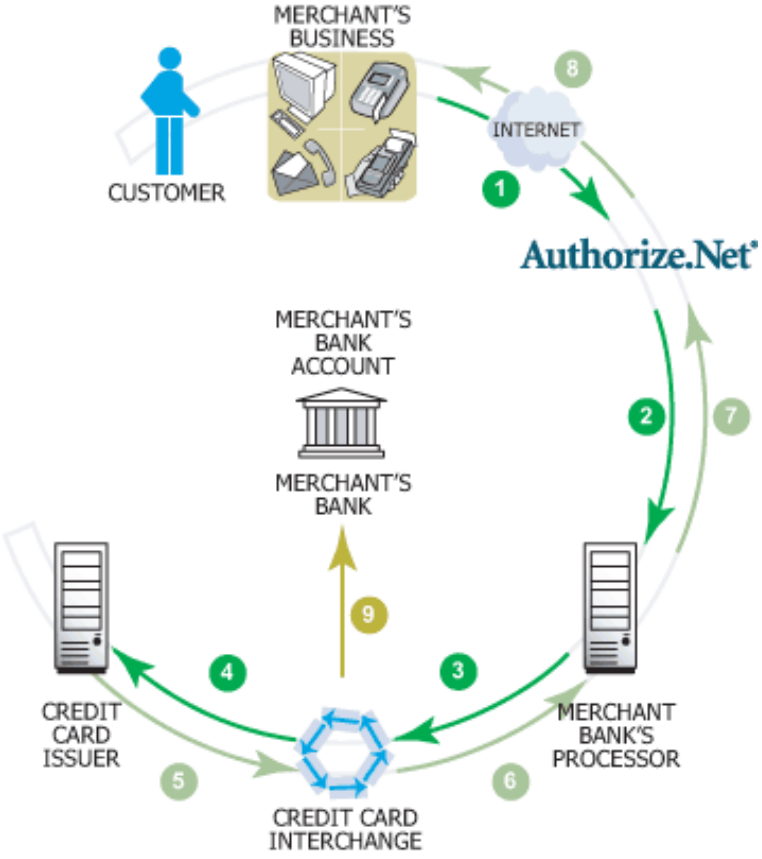
Click ***Help*** to the **Online Help** window and then click the hyperlink of the items to get the information.



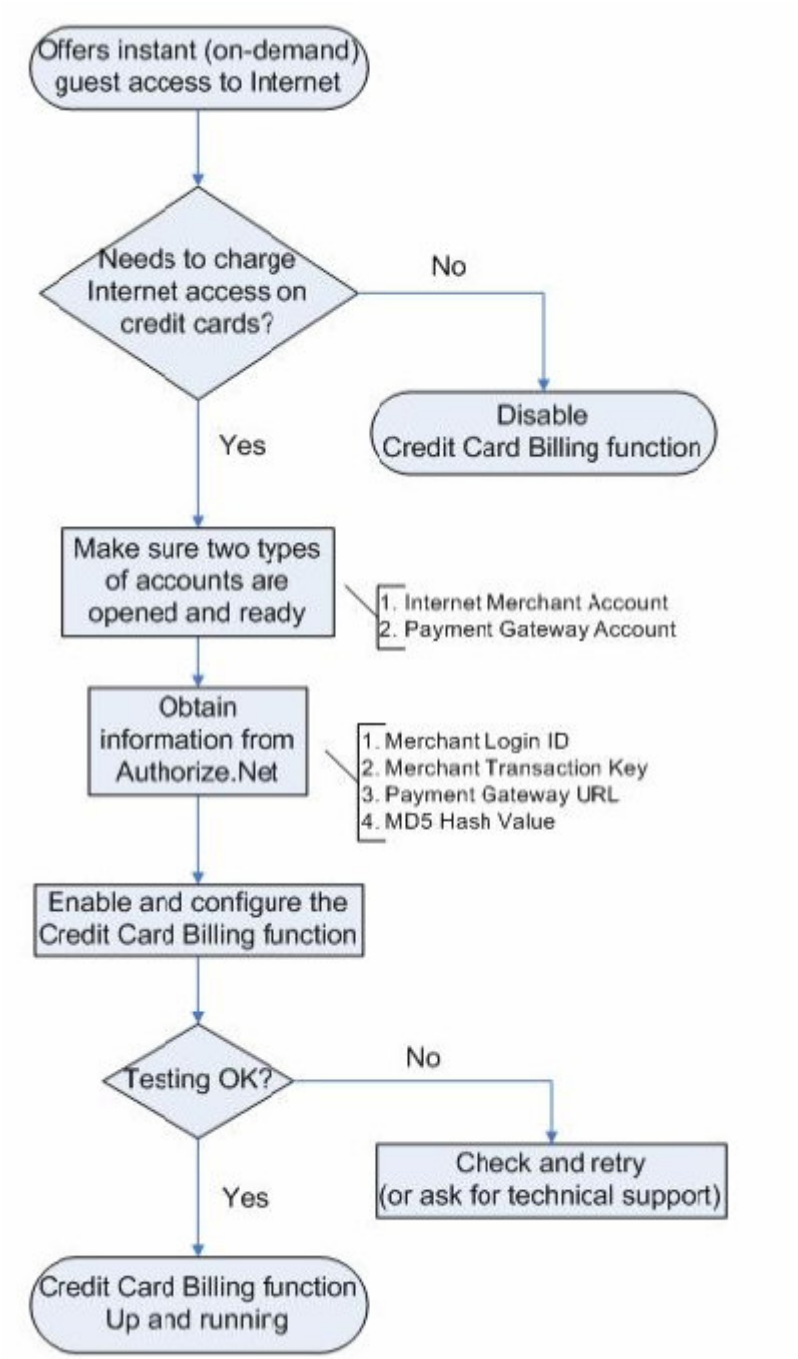
© 2008 4IPNET, INC.

Appendix A. Accepting Payment via Authorize.Net

This section is to show independent Hotspot owners how to configure related settings in order to accept credit card payments via Authorize.Net, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their credit cards.



© 2008 4IPNET, INC.


Offers instant (on-demand) guest access to Internet
Needs to charge Internet access on credit cards?
No
Disable Credit Card Billing function
Yes
Make sure two types of accounts are opened and ready
1. Internet Merchant Account
2. Payment Gateway Account
Obtain information from Authorize.Net
1. Merchant Login ID
2. Merchant Transaction Key
3. Payment Gateway URL
4. MD5 Hash Value
Enable and configure the Credit Card Billing function
Testing OK?
No
Check and retry (or ask for technical support)
Yes
Credit Card Billing function Up and runnirg

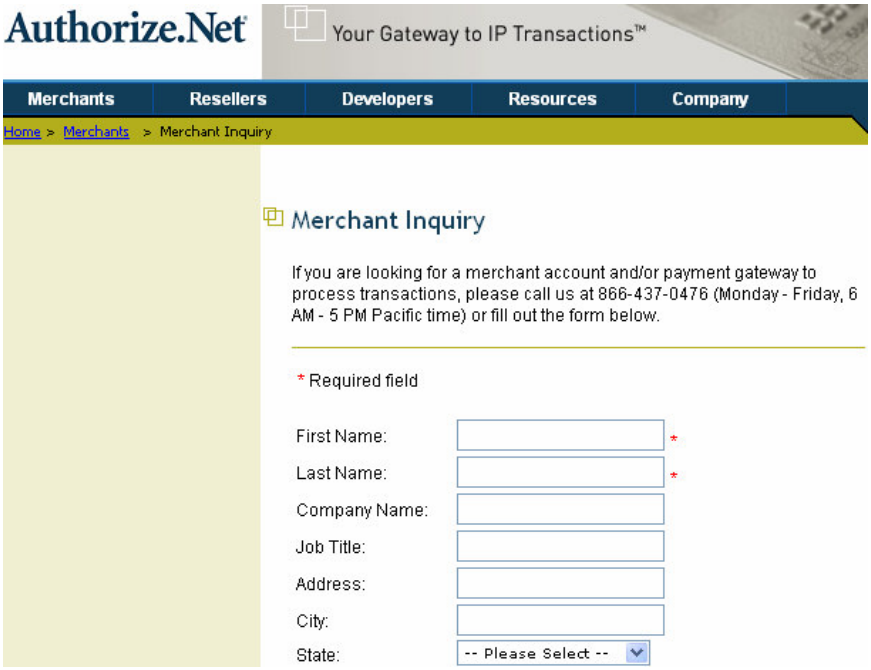
© 2008 4IPNET, INC.

1. Setting Up

1.1 Open Accounts

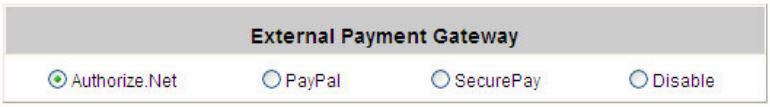
To set up 4ipnet WHG303 to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account).

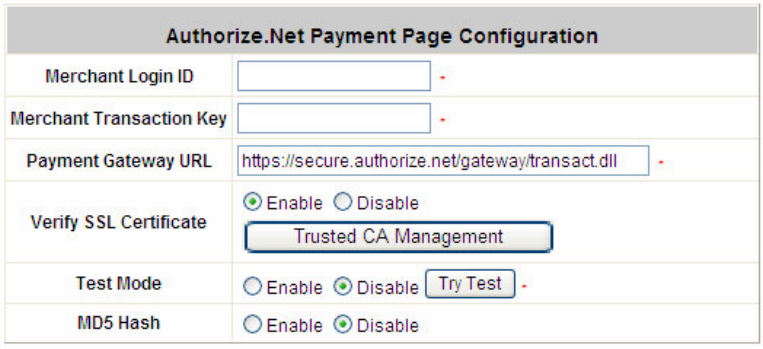
If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/.



1.2 Configure 4ipnet WHG303 using an Authorize.Net account

Please log in 4ipnet WHG303. **User Authentication** >> **Authentication Configuration** >> Click the server name ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.Net***





© 2008 4IPNET, INC.

Some major fields are required:

Setting	Description
Merchant Login ID	This is the "Login ID" that comes with the Authorize.Net account.
Merchant Transaction Key	To get a new key, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **Obtain Transaction Key** >> Enter **"Secret Answer"** >> Click ***Submit.***
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll (default gateway address)
MD5 Hash	To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: **"MD5 Hash Value"**.

Note: For detailed description, please see ***4.2.1.6 Authentication Method – On-demand User.***

1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of 4ipnet WHG303

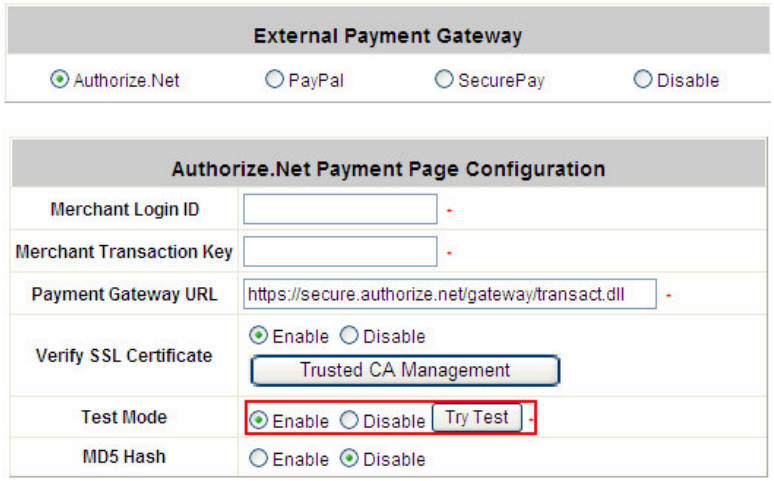
Settings of the merchant account on Authorize.Net should be matched with the configuration of 4ipnet WHG303:

Setting	Description
MD5 Hash	To configure **"MD5 Hash Value"**, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **MD5 Hash** >> Enter **"New Hash Value"** & **"Confirm Hash Value"** >> Click ***Submit***.
Required Card Code	If the **"Card Code"** is set up as a required field, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **Card Code Verification** >> Check the **Does NOT Match (N)** box >> Click ***Submit***.
Required Address Fields	After setting up the required address fields on the **"Credit Card Payment Page Billing Configuration"** section of 4ipnet WHG303, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **Address Verification System (AVS)** >> Check the boxes accordingly >> Click ***Submit***.

1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between 4ipnet WHG303 and Authorize.Net, please log in 4ipnet WHG303. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.Net*** >> Go to "**Authorize.Net Payment Page Configuration**" section >> ***Enable*** the **"Test Mode"** >> Click ***Try Test*** and follow the instructions

© 2008 4IPNET, INC.



2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as 4ipnet WHG303.

2.1 Void A Transaction and Remove the On-demand Account Generated on 4ipnet WHG303

Sometimes, a transaction (as well as the related user account on 4ipnet WHG303) may have to be canceled before it has been settled with the bank.

a. To void an unsettled transaction, please log in Authorize.Net. Click **Unsettled Transactions** >> Locate the specific transaction record on the **"List of Unsettled Transactions"** >> Click the **Trans ID** number >> Confirm and click **Void**.

Note: To find the on-demand account name, click ***Show Itemized Order Information*** on the **"Order Information"** page >> Username can be found in the **"Item Description"**.

b. To remove the specific account from 4ipnet WHG303, please log in 4ipnet WHG303. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List** >> Click ***Delete*** on the record with the account name. Click ***Delete All*** to delete all users at once.

2.2 Refund A Settled Transaction and Remove the On-demand Account Generated on 4ipnet WHG303

a. To refund a credit card payment, please log in Authorize.Net. Click **Virtual Terminal** >> Select a Payment Method >> Click **Refund a Credit Card** >> **Payment/Authorization Information** >> Type information in at least three fields: **Card Number**, **Expiration Date**, and **Amount** >> Confirm and click ***Submit***.

© 2008 4IPNET, INC.

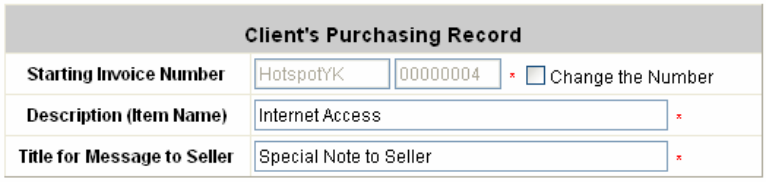
b. To remove the specific account from 4ipnet WHG303, please log in 4ipnet WHG303. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List** >> Click ***Delete*** on the record with the account name.

2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click **Unsettled Transactions** >> Try to locate the specific transaction record on the **"List of Unsettled Transactions"** >> Click the **Trans ID** number >> Click **Show Itemized Order Information** in the **"Order Information"** section >> Username and Password can be found in the **"Item Description"**.

2.4 Send An Email Receipt to A Customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via Authorize.Net. To change the information on the receipt for customer, please log in 4ipnet WHG303. **User Authentication** >> **Authentication Configuration** >> Click the server **On-demand User** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.NET*** >> Scroll down to **Client's Purchasing Record** section of the page >> Type in information in the text boxes: "**Description" and "E-mail Header"** >> Confirm and click ***Apply***.



2.5 Send an Email Receipt for Each Transaction to the Merchant Owner

A copy of email receipt with payment details for each successful transaction will also be automatically sent to the merchant owner/administrator via Authorize.Net.

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click **Settings and Profile** >> Go to the **"General"** section >> Click **Manage Contacts** >> Click **Add New Contact** to >> Enter necessary contact information on this page >> Check the **"Transaction Receipt"** box >> Click ***Submit***.

© 2008 4IPNET, INC.

3. Reporting

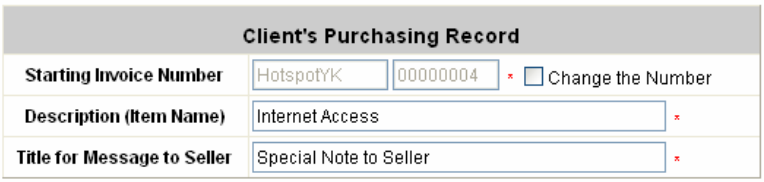
During normal operation, the following steps will be necessary to generate transaction reports.

3.1 Transaction Statistics by Credit Card Type during the Period.

Please log in Authorize.Net. >> Click **Reports** >> Check **"Statistics by Settlement Date"** radio button >> Select **"Transaction Type"**, **"Start Date"**, and **"End Date"** as the criteria >> Click ***Run Report***.

3.2 Transaction Statistics by Different Location

a. To deploy more than one 4ipnet WHG303, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in 4ipnet WHG303. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.NET*** >> Scroll down to **"Client's Purchasing Record"** section of the page >> Check the **"Reset"** box >> A location-specific ID (for example, Hotspot-A) can be used as the first part of **"Invoice Number"** >> Confirm and click ***Apply***.



b. Please log in Authorize.Net >> Click **Search and Download** >> Specify the transaction period (or ALL Settled,
c. Unsettled) in **"Settlement Date"** section >> Go to **"Transaction"** section >> Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A*) in the **"Invoice #"** text box >> Click ***Search*** >> If transaction records can be found, the number of accounts sold is the number of search results >> Or, click **Download To File** to download records and then use MS Excel to generate more detailed reports.

3.3 Search for The Transaction Details for A Specific Customer

Please log in Authorize.Net. Click **Search and Download** >> Enter the information for a specific customer as criteria >> Click ***Search*** >> Click the **Trans ID** number to view the transaction details.

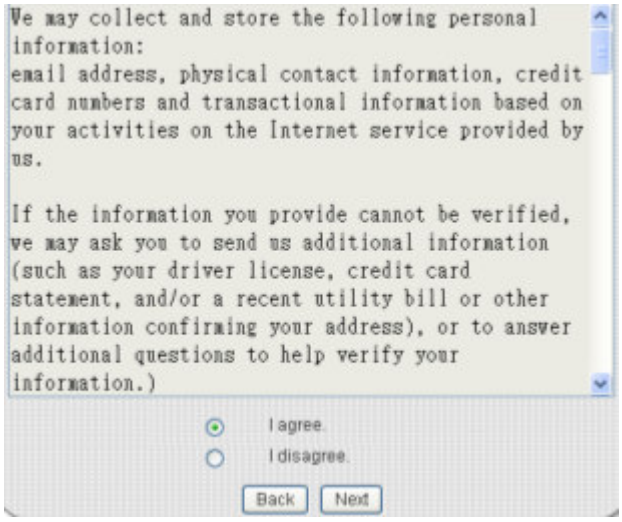
Note: For more information about **Authorize.Net**, please see **http://www.authorize.net**.

© 2008 4IPNET, INC.

4. Examples of Making Payment for End Users

Step 1: Click the link below the login window to pay for the service by credit card via Authorize.Net.

Step 2: Choose ***I agree*** to accept the terms of use and click ***Next***.


We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)
I agree
I disagree
Back
Next

© 2008 4IPNET, INC.

Step 3: Please fill out the form and Click ***Submit*** to send out this transaction. There will be a confirm dialog box.

Step 4: Please confirm the data and the click ***OK*** to go on the transaction or click ***Cancel*** to revise the data or cancel this transaction. After clicking OK, there will be another dialog box showing up to confirm this transaction again.

© 2008 4IPNET, INC.

Step 5: Click ***OK*** to complete the process or click ***Cancel*** to revise the data or cancel this transaction.

Microsoft Internet Explorer
The process may take several minnutes.
Please DO NOT close or leave this page before getting the result.
Do you want to continue the credit card payment process?
OK
Cancel

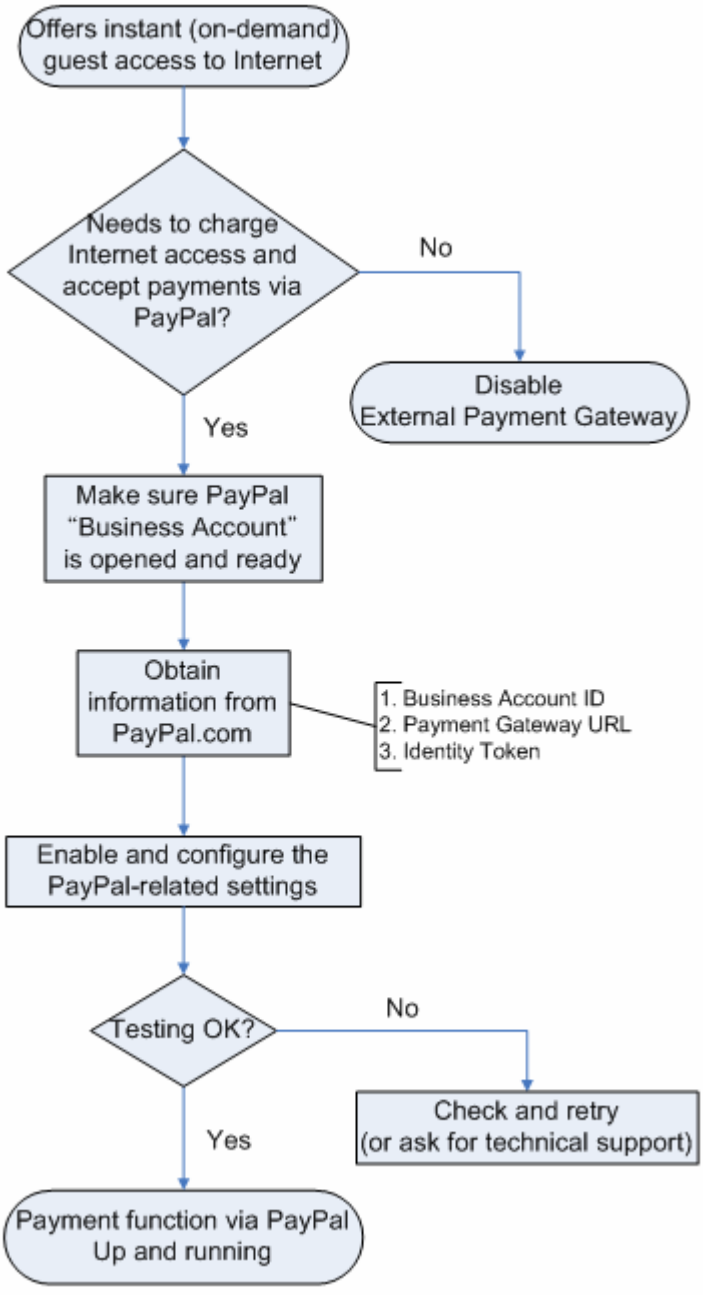
Step 6: Click ***Start Internet Access*** to use the Internet access service.

Note: The clients must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If clients choose to enter the e-mail addresses, clients will receive confirmation letters for reference.

© 2008 4IPNET, INC.

Appendix B. Accepting Payment via PayPal

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via PayPal, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their PayPal accounts or credit cards.


Offers instant (on-demand) guest access to Internet
Needs to charge Internet access and accept payments via PayPal?
No
Disable External Payment Gateway
Yes
Make sure PayPal "Business Account" is opened and ready
Obtain information from PayPal.com
1. Business Account ID
2. Payment Gateway URL
3. Identity Token
Enable and configure the PayPal-related settings
Testing OK?
No
Check and retry (or ask for technical support)
Yes
Payment function via PayPal Up and running

© 2008 4IPNET, INC.

1. Setting Up

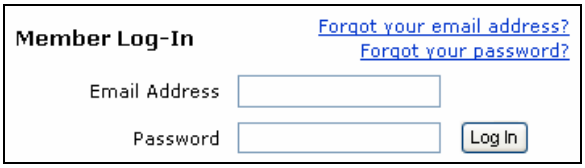
As follows are the basic steps to open and configure a "**Business Account**" on **PayPal**.

1.1 Open An Account

Step 1: Sign up for a PayPal Business Account and login.

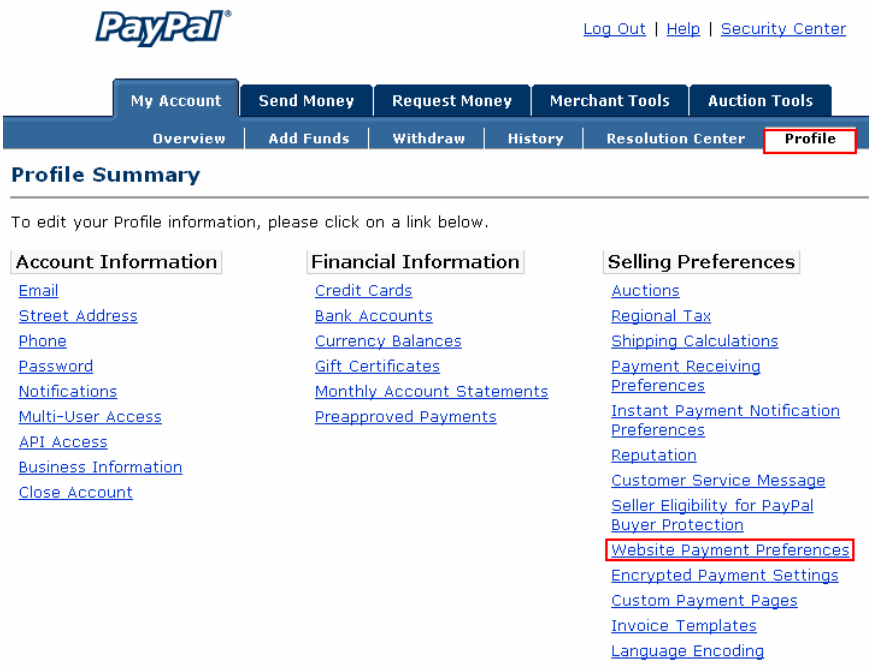
Here is a link: https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run

Choose Account Type → Enter Information → Confirm → Done
Sign Up for a PayPal Account
Anyone with an email address can use PayPal to send and receive money online. What is PayPal?
Already have a PayPal Account?
Upgrade your account
Personal Account
Ideal for shopping online. It's a free, secure, and fast way to send payments. You can also accept bank account or PayPal balance-funded payments for free and a limited number of credit or debit card payments per year for a low fee. Learn more
Premier Account
Perfect for buying and selling on eBay or merchant websites. Accept all payment types for low fees. Do business under your own name.
Business Account
The right choice for your online business. Accept all payment types for low fees. Do business under a company or group name. Learn more



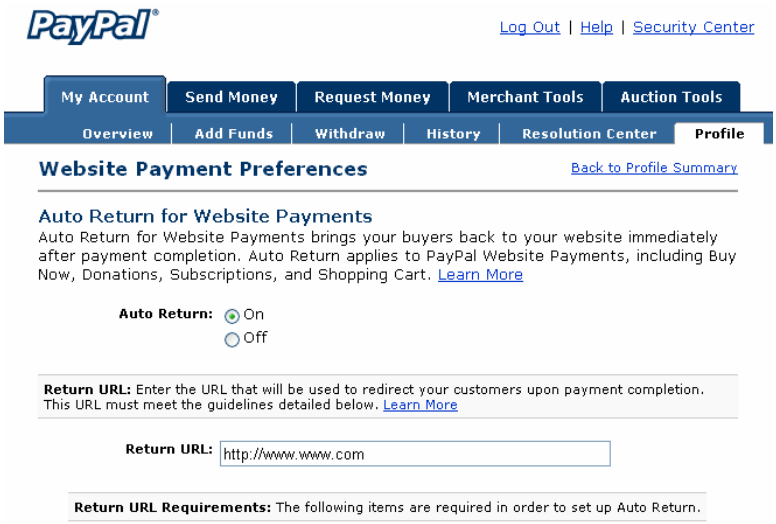
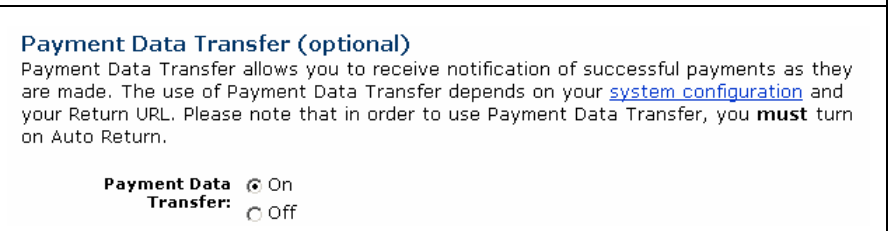
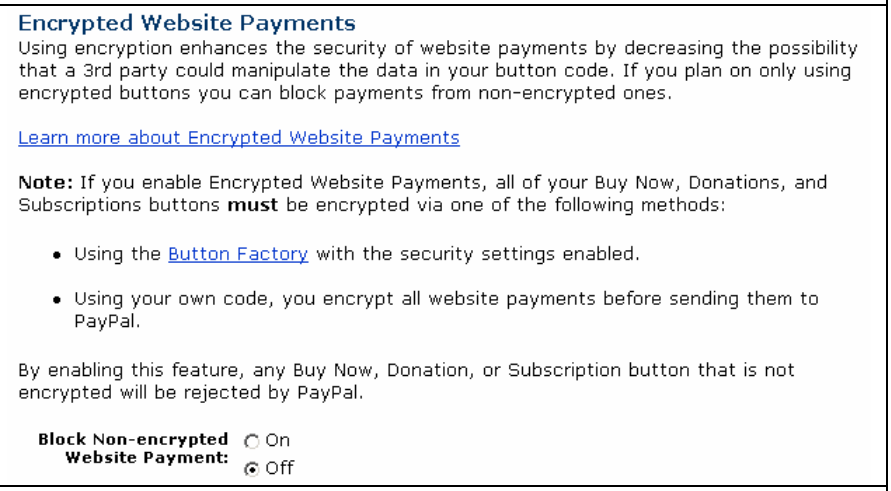
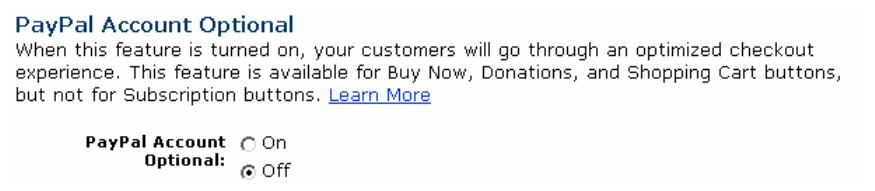
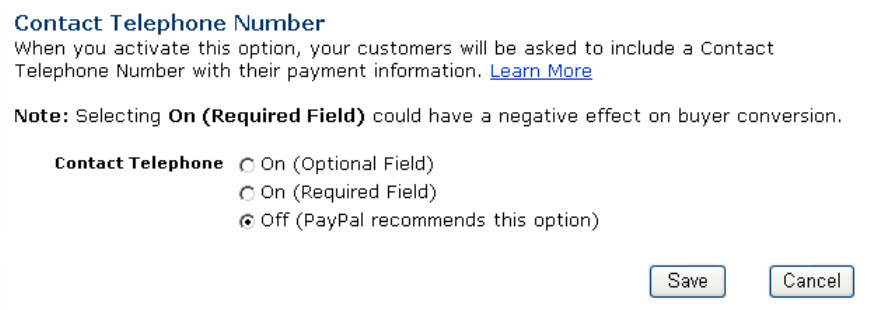
Step 2: Edit necessary settings in "Website Payment Preferences"

Click **Profile** >> Click **Website Payment Preferences** in the **Selling Preferences** section



Administrators should scroll down to edit each setting as shown in the table below. To activate all the changes, please click ***Save*** at the end of the page.

© 2008 4IPNET, INC.

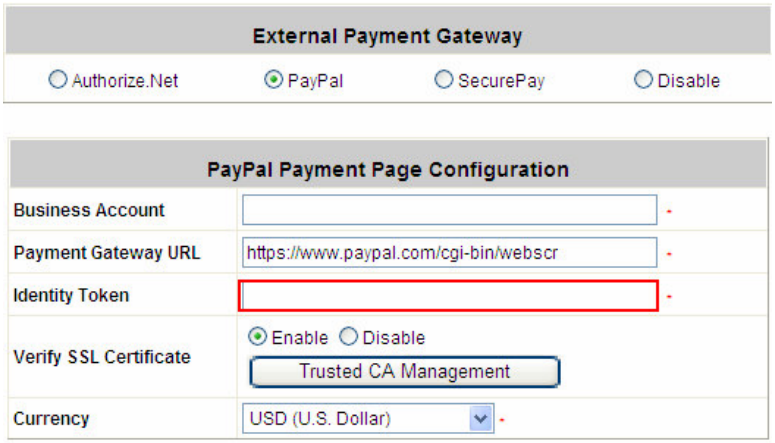
Settings	Screenshots
Auto Return (On) **Return URL (Redirect Webpage)** Type http://www.www.com or other URL.	
Payment Data Transfer (On)	
Block Non-encrypted Website Payment (Off)	
PayPal Account Optional (Off)	
Contact Telephone Number (Off) **Click *Save.***	

© 2008 4IPNET, INC.

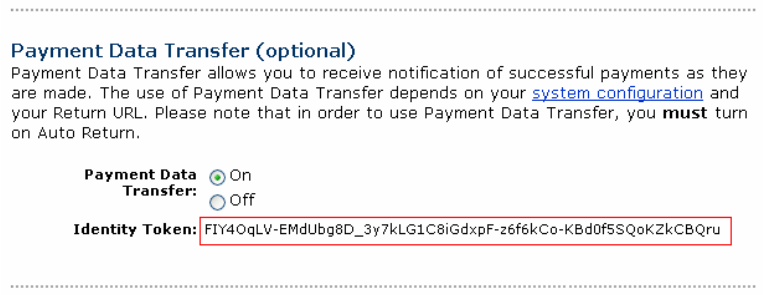
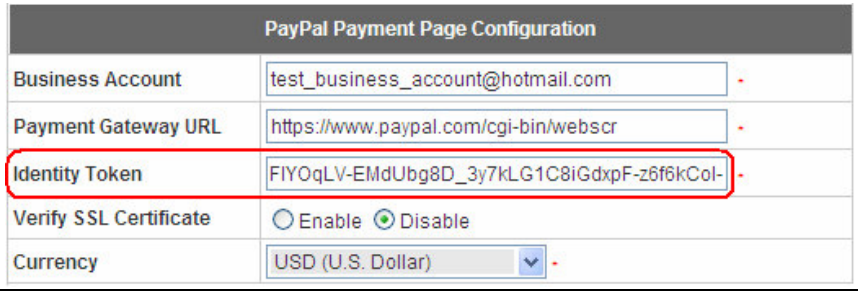
1.2 Configure 4ipnet WHG303 with a PayPal Business Account

Please log in 4ipnet WHG303:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***PayPal***



Three fields are required:

Setting	Description
Business Account ID	This is the "Login ID" (email address) that is associated with the PayPal Business Account.
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr (default URL for PayPal)
Identity Token	Please log in PayPal after saving the above settings >> Click **Profile** >> Click **Website Payment Preferences** in the **Selling Preferences** section >> Scroll down to the section, **Payment Data Transfer (optional)**.  Copy the **Identity Token** in the above page to the section "**PayPal Payment Page Configuration**" of 4ipnet WHG303. 

© 2008 4IPNET, INC.

1.3 Requirements for Building a Secure PayPal-based E-Commerce Site

To deploy the PayPal function properly, it is required that the merchant register an **Internet domain name** (for example, www.StoreName.com) for this subscriber gateway device.

In addition, it is necessary to sign up for a **SSL certificate**, licensed from a "**Certificate Authority**" (for example, **VeriSign**), for this registered Internet domain name.

Thus, by meeting these two requirements, it will allow end customers or subscribers to pay for the Internet access in a securer and convenient way.

2. Basic Maintenance

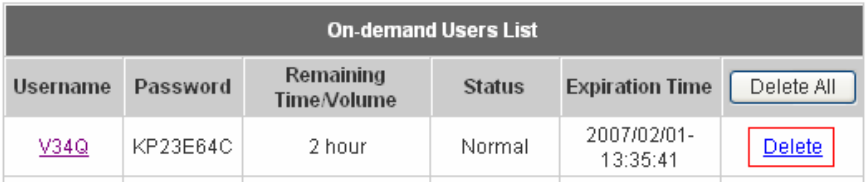
In order to maintain the operation, the merchant owner will have to manage the accounts and payment transactions on PayPal website as well as 4ipnet WHG303.

2.1 Refund a completed payment and remove the on-demand account generated on 4ipnet WHG303

(1) To refund a payment, please log in PayPal >> Click **History** >> Locate the specific payment listing in the activity history log >> Click **Details** of the payment listing >> Click **Refund Payment** at the end of the details page >> Type in information: **Gross Refund Amount** and/or **Optional Note to Buyer** >> Click ***Submit*** >> Confirm the details and click ***Process Refund***

(2) To remove the specific account from 4ipnet WHG303, please log in 4ipnet WHG303:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List** >> Click ***Delete*** on the record with the account ID. Click ***Delete All*** to delete all users at once.



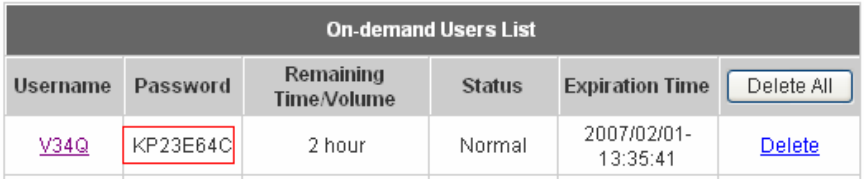
© 2008 4IPNET, INC.

2.2 Find the username and password for a specific customer

(1) To find the username, please log in PayPal >> Click **History** >> Locate the specific payment listing in the activity history log >> Click **Details** of the payment listing >> Username can be found in the **"Item Title"** field

(2) To find the password associated with a specific username, please log in 4ipnet WHG303:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List**. Search for the specific username. Password can be found in the same record



On-demand Users List

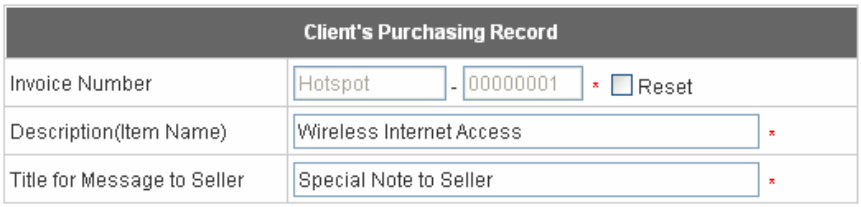
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
V34Q	KP23E64C	2 hour	Normal	2007/02/01-13:35:41	Delete

Note: As stated by PayPal, you can issue a full or partial refund for any reason and for **60 days** after the original payment was sent. To find the on-demand account name for a specific payment, click ***Details*** of the payment listing in the activity history log >> **Username** can be found in the **"Item Title"** field.

2.3 Send an email receipt to a customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via PayPal. To change the information on the receipt for customer, please log in 4ipnet WHG303:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand User Server Configuration** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***PayPal*** >> Go to "**Client's Purchasing Record**" section >> Type in information in the text boxes: **Invoice Number** and **Description (Item Name)** >> Confirm and click ***Apply***



Client's Purchasing Record

Invoice Number	Hotspot - 00000001 * Reset
Description(Item Name)	Wireless Internet Access *
Title for Message to Seller	Special Note to Seller *

2.4 Send an email receipt for each transaction to the merchant

A copy of email receipt with payment details (including available message note from buyer) for each successful transaction will also be automatically sent to the merchant owner/administrator via PayPal.

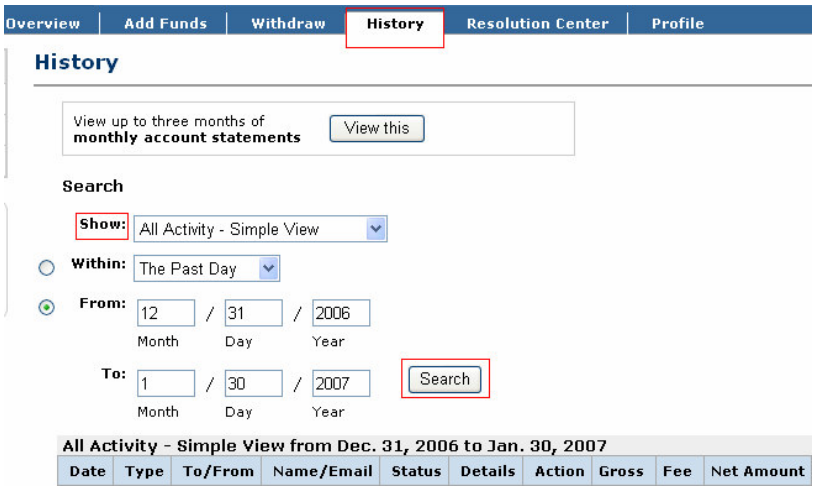
© 2008 4IPNET, INC.

3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

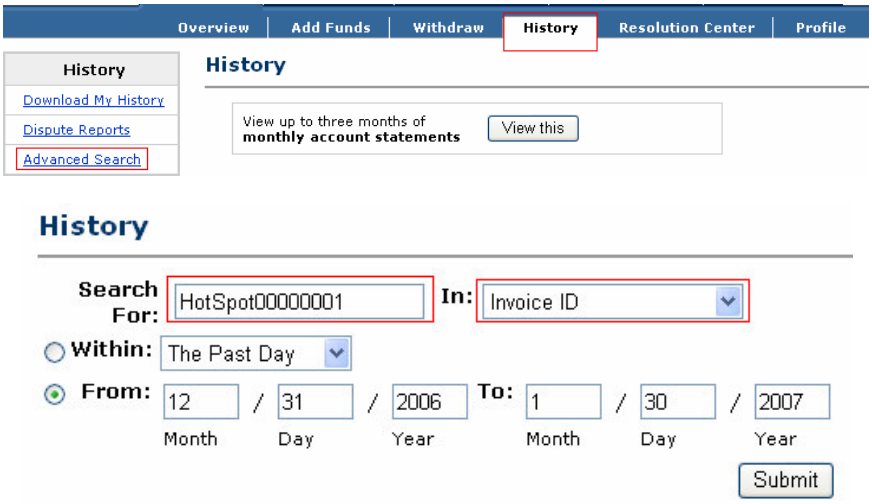
3.1 Transaction activity during a period

(1) Please log in PayPal >> Click **History** >> Choose activity type from the **Show** field as the search criteria >> Specify the dates (**From** and **To** fields) for the period >> Click ***Search***



3.2 Search for the transaction details for a specific customer

Please log in PayPal >> Click **History** >> Click **Advanced Search** >> Enter the name for a specific customer as criteria in the **Search For** field and Choose Last Name or First Name in the **In** field >> Specify the time period >> Click ***Submit*** >> Click **Details** to view the transaction details



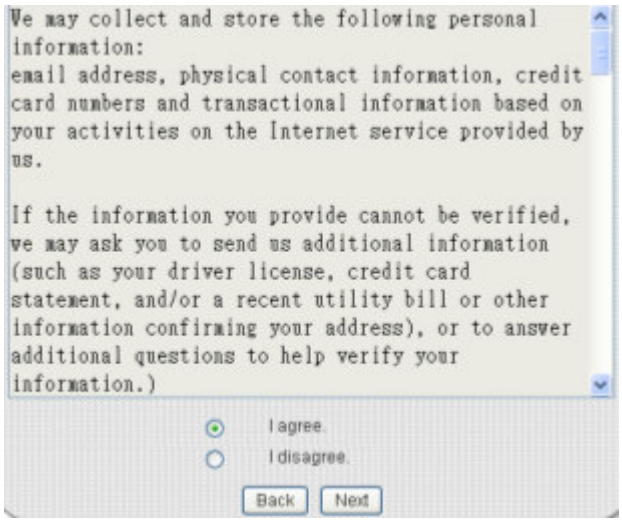
Note: For more information about **PayPal**, please see **http://www.paypal.com**.

© 2008 4IPNET, INC.

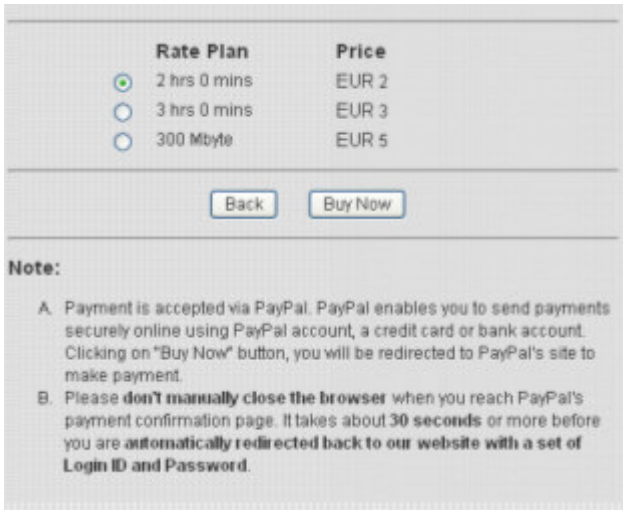
4. Examples of Making Payment for End Users

Step 1: Click the link below the login window to pay for the service via PayPal.

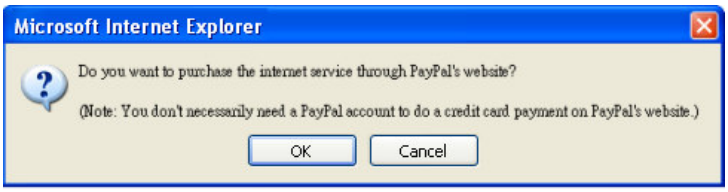
Step 2: Choose ***I agree*** to accept the terms of use and click ***Next***.


We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)
I agree.
I disagree.
Back
Next

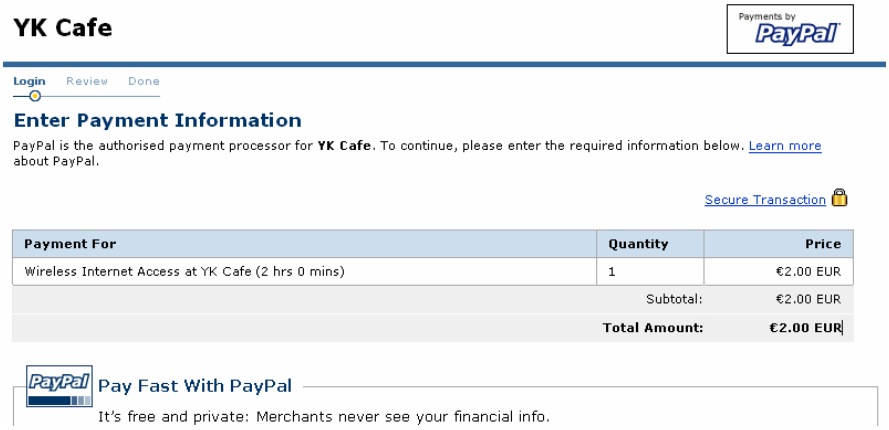
Step 3: Please fill out the form and Click ***Submit*** to send out this transaction. There will be a confirm dialog box.

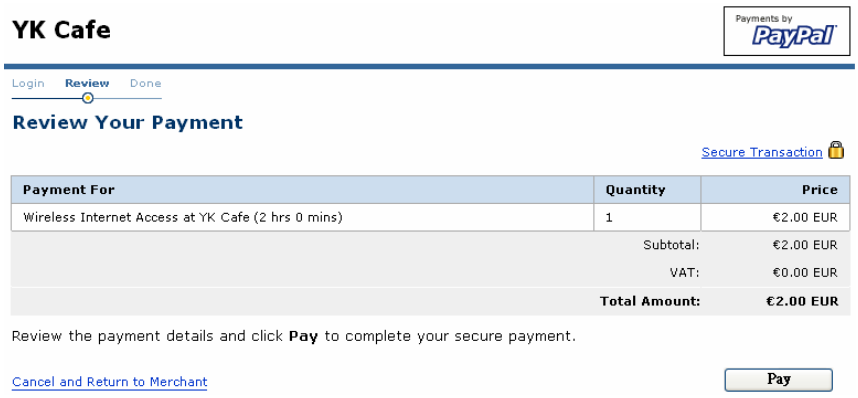

Rate Plan
Price
2 hrs 0 mins
EUR 2
3 hrs 0 mins
EUR 3
300 Mbyte
EUR 5
Back
Buy Now
Note:
A. Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button, you will be redirected to PayPal's site to make payment.
B. Please don't manually close the browser when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are automatically redirected back to our website with a set of Login ID and Password.

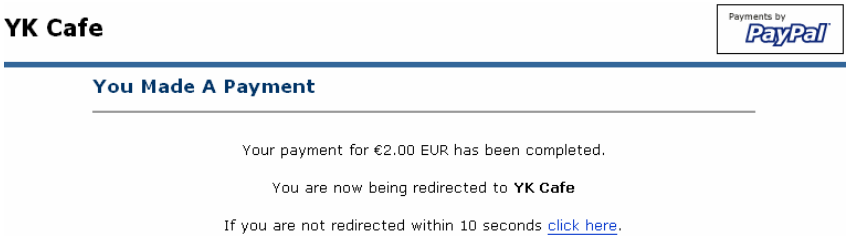
© 2008 4IPNET, INC.


Microsoft Internet Explorer
Do you want to purchase the internet service through PayPal's website?
(Note: You don't necessarily need a PayPal account to do a credit card payment on PayPal's website.)
OK
Cancel

Step 4: You will be redirected to PayPal website to complete the payment process.

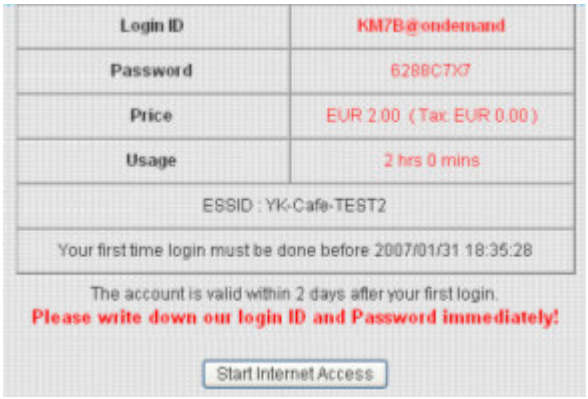

YK Cafe
Payments by PayPal
Login Review Done
Enter Payment Information
PayPal is the authorised payment processor for YK Cafe. To continue, please enter the required information below. Learn more about PayPal.
Secure Transaction
Payment For
Quantity
Price
Wireless Internet Access at YK Cafe (2 hrs 0 mins)
1
€2.00 EUR
Subtotal:
€2.00 EUR
Total Amount:
€2.00 EUR
Pay Fast With PayPal
It's free and private: Merchants never see your financial info.




YK Cafe
Payments by PayPal
You Made A Payment
Your payment for €2.00 EUR has been completed.
You are now being redirected to YK Cafe
If you are not redirected within 10 seconds click here.

© 2008 4IPNET, INC.

Step 5: Click ***Start Internet Access*** to use the Internet access service.


Login ID
KM7B@ondemand
Password
6288C7X7
Price
EUR 2.00 (Tax EUR 0.00)
Usage
2 hrs 0 mins
ESSID : YK-Cafe-TEST2
Your first time login must be done before 2007/01/31 18:35:28
The account is valid within 2 days after your first login.
Please write down our login ID and Password immediately!
Start Internet Access

Note:

(a) Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on ***Buy Now*** button, you will be redirected to PayPal's site to make payment.

(b) Please **do not manually close the browser** when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are **automatically redirected back to our website with a set of Login ID and Password**.

© 2008 4IPNET, INC.

Appendix C. Accepting Payment via SecurePay

▪ How to use SecurePay

SecurePay is another external online payment gateway compatible with WHG303. This section guides you how to get SecurePay working with WHG303 and how to check today's billing transactions, and teaches your clients how to purchase or renew different network-access plans online using their credit cards.

▪ For Administrators to get started

Before getting started, administrators need to apply for a "Merchant ID" and "Merchant Password" from the "SecurePay" official website.

In this example, merchant account one starting with plan one is

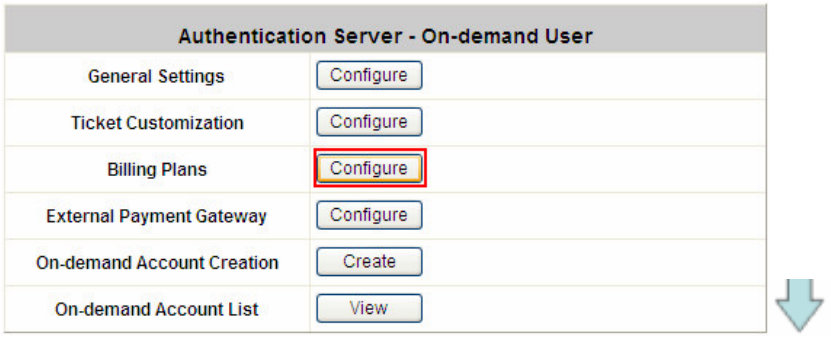
SecurePay Merchant *ID*: ABC0001

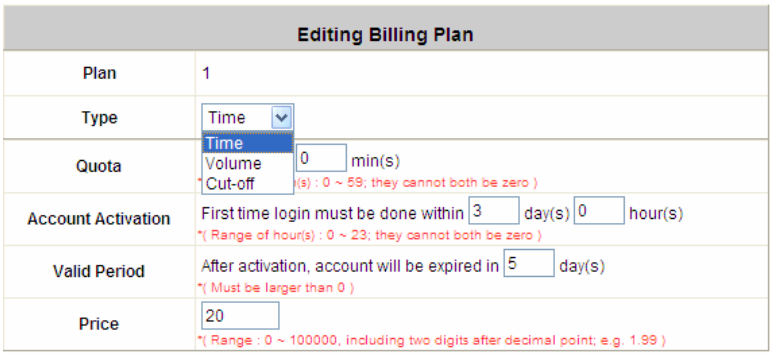
SecurePay Merchant *Password*: abc123

1. Create billing plans:

Administrators may come up with many ways to charge their clients. For example:

➢ Plan 1 (charged by Time): Each Plan 1 client has to make their first login within 3 days. The user can access the internet for 2 hours and this account is valid for 5 days. He's being charged 20 dollars for this plan.



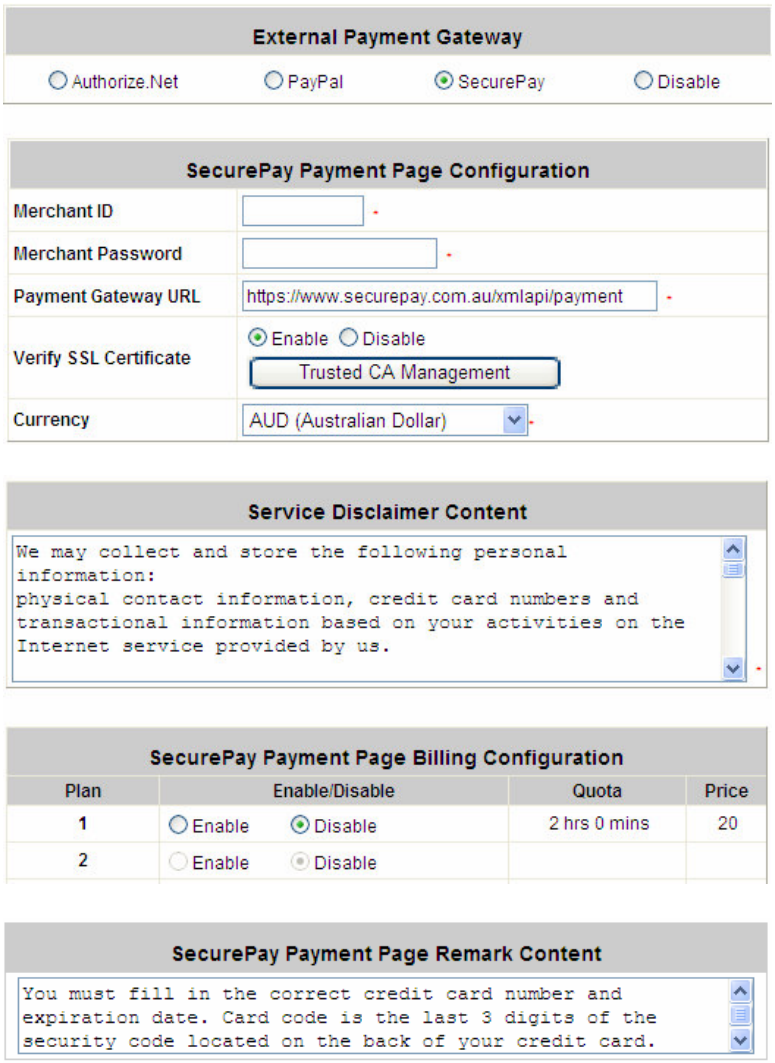


© 2008 4IPNET, INC.

2. Payment Configuration:

Select "Secure Pay" for your external payment gateway. Enter Merchant ID and Password. And Payment Gateway URL is one fixed URL: https://www.securepay.com.au/xmlapi/payment.

Finally, enable whichever plan(s) you'd like to apply to "SecurePay".

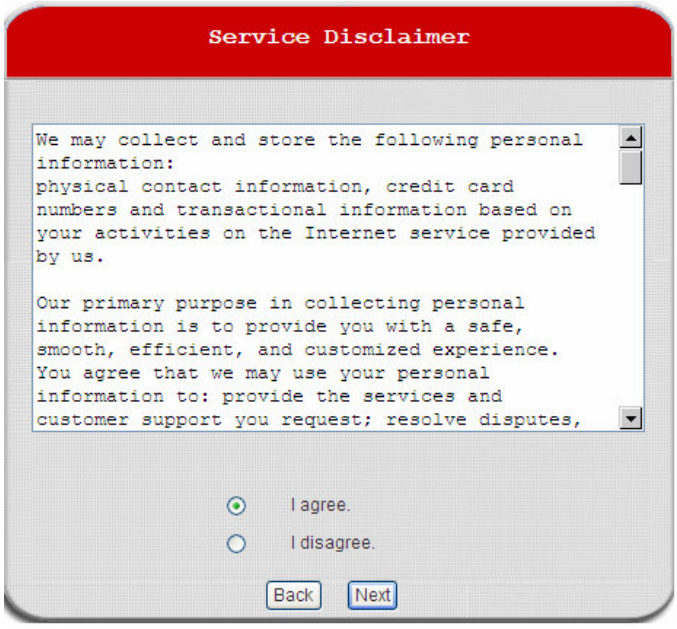


© 2008 4IPNET, INC.

▪ How does your client purchase a plan?

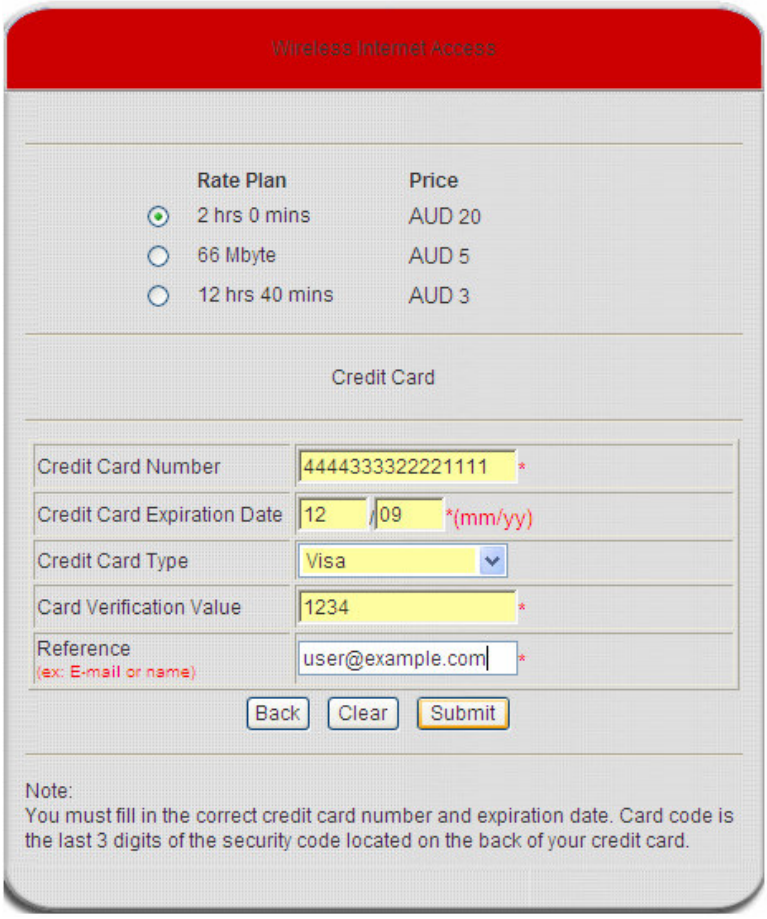
1. Open a browser, it then shows a login page. And click "***Click here to purchase by Credit Card online***" to get started.

2. Select "***I agree***" and click "***Next***".


Service Disclaimer
We may collect and store the following personal information:
physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
Our primary purpose in collecting personal information is to provide you with a safe, smooth, efficient, and customized experience. You agree that we may use your personal information to: provide the services and customer support you request; resolve disputes,
I agree.
I disagree.
Back
Next

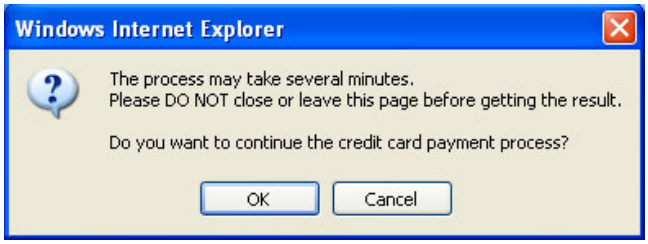
© 2008 4IPNET, INC.

3. Select a billing plan to purchase; enter your credit card information and "***Submit***".



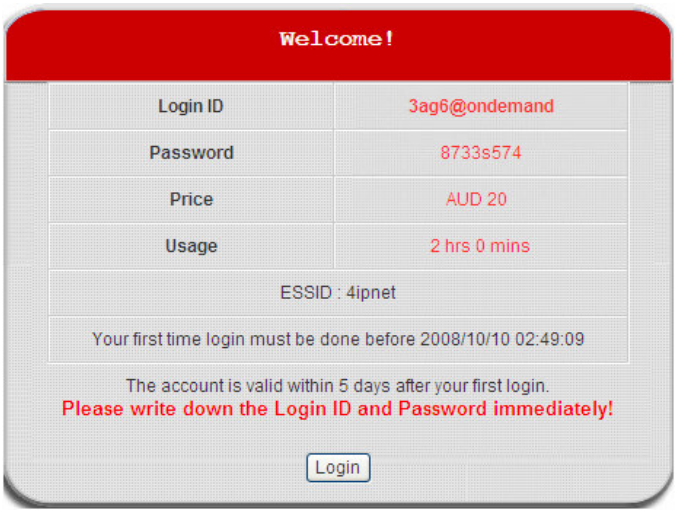
4. Double confirm your credit card information.

5. Double confirm with your purchase. And wait for a couple minutes till you get your receipt.

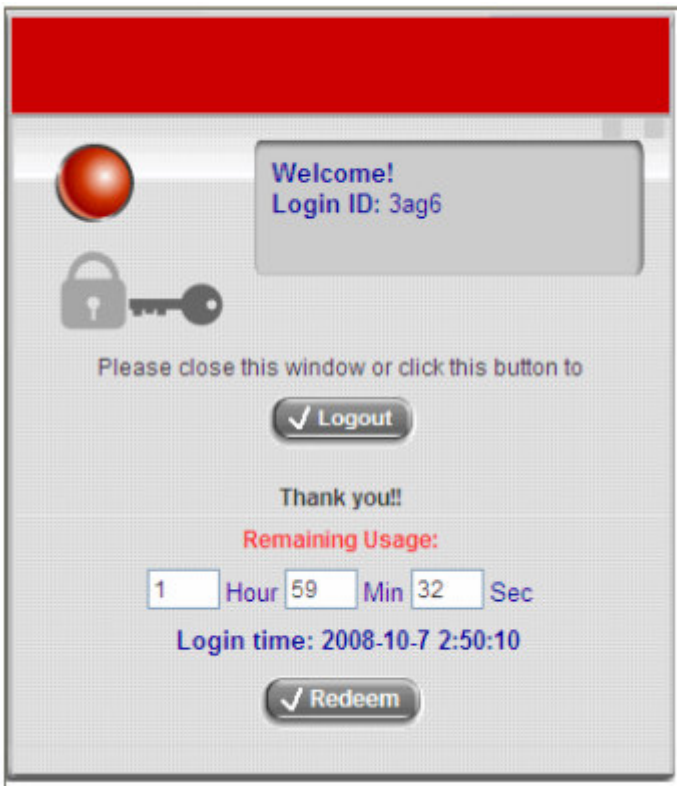

Windows Internet Explorer
The process may take several minutes.
Please DO NOT close or leave this page before getting the result.
Do you want to continue the credit card payment process?
OK
Cancel

© 2008 4IPNET, INC.

6. Account has been successfully generated! Click "***Login***". And it's recommended not to close this page at all times in case you might re-login.

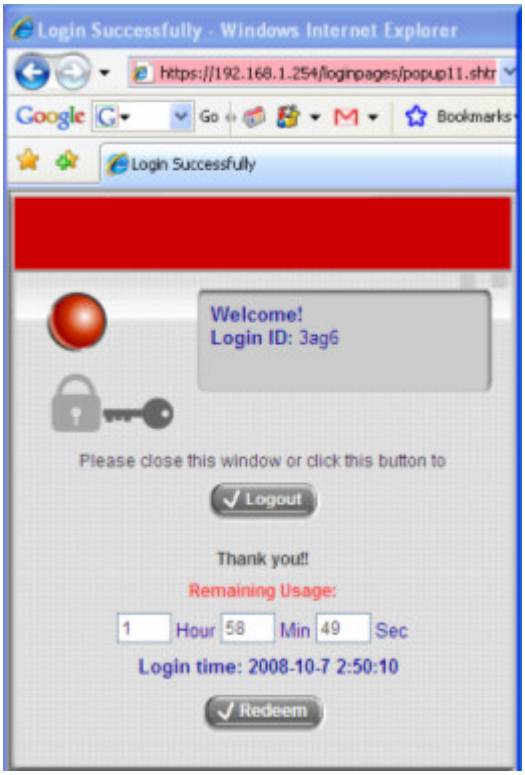


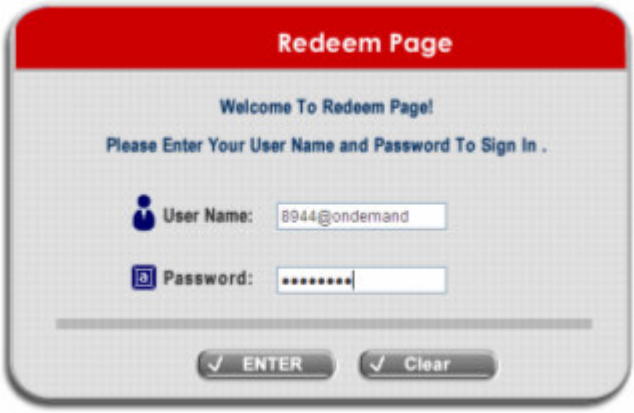
7. The login successful box appears. Click "***Start Browsing***" to get online.



© 2008 4IPNET, INC.

8. User is now redirected to YOUR homepage that URL you fill in the blank "**System Configuration >> Homepage**".



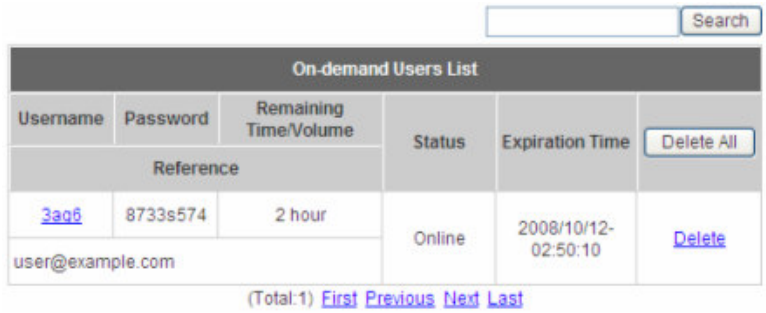


© 2008 4IPNET, INC.

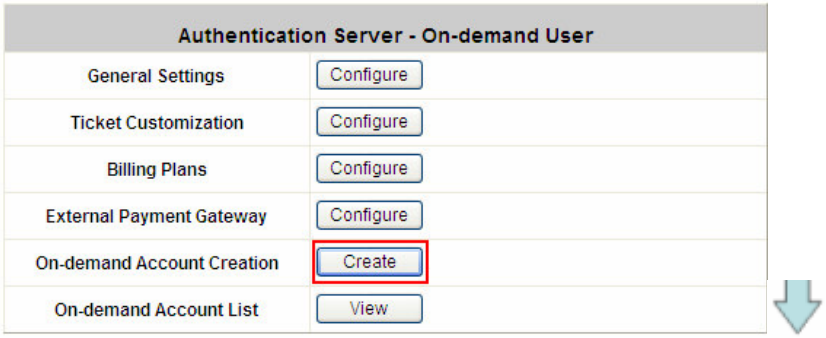
▪ How does your client renew his service after running out of quota?

New username and password are needed to renew service. Client can either purchase a new account online (shown in the last section) or at the counter desk. The following example is to enter Web UI, manually generate an account and have your client renewed himself the service.

1. Go to On-demand Users List, the account being generated online (please see the last section) is shown.



2. Create an on-demand user.



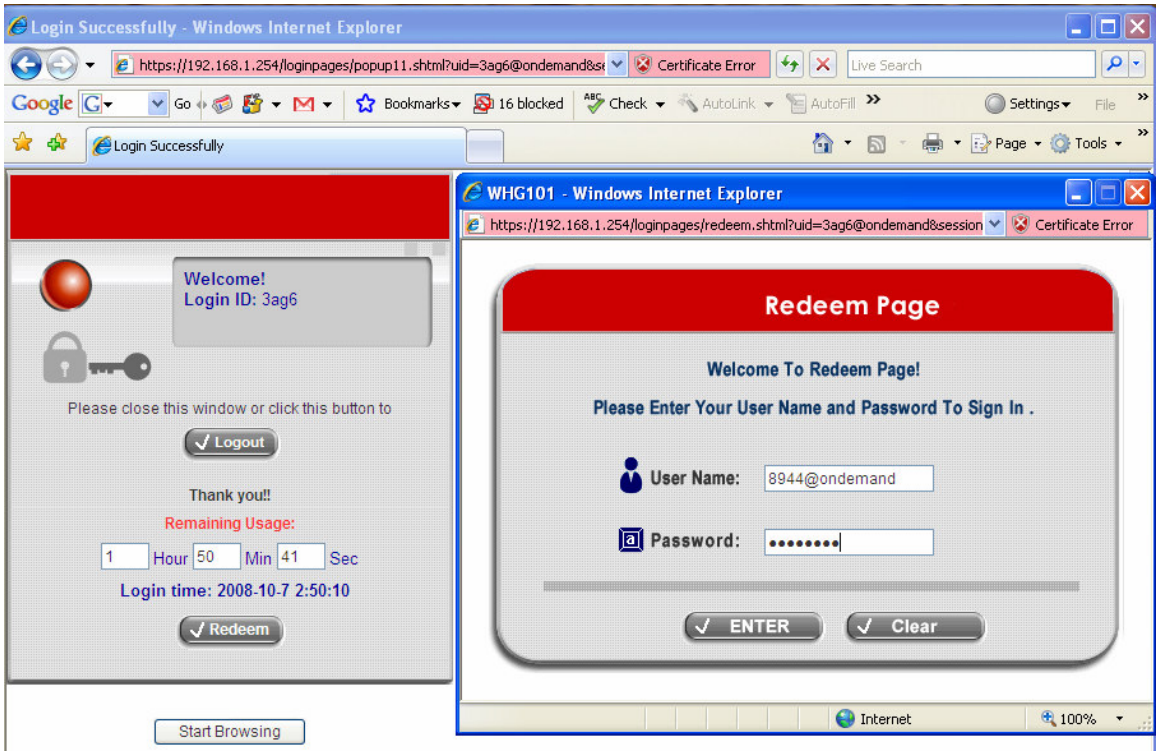
3. Choose a billing plan for this user and click "***Create***".

4. Give your client the print-out of this receipt with new account information.

© 2008 4IPNET, INC.

Username	8944@ondemand
Password	85cb898e
Price	AUD 3
Usage	12 hrs 40 mins
ESSID : 4ipnet	
Wireless Key :	
You first time login must be done before 2008/10/10 17:56:18	
The account is valid within 8 days after your first login.	

5. Have your client go back to the "Login successful page" and click "***Redeem***". And enter new **User Name** and **Password**.



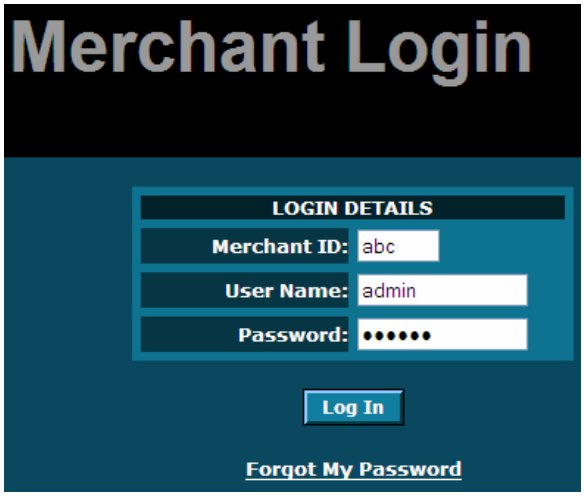
© 2008 4IPNET, INC.

6. Redeem is successful and you can see more quota for internet access.

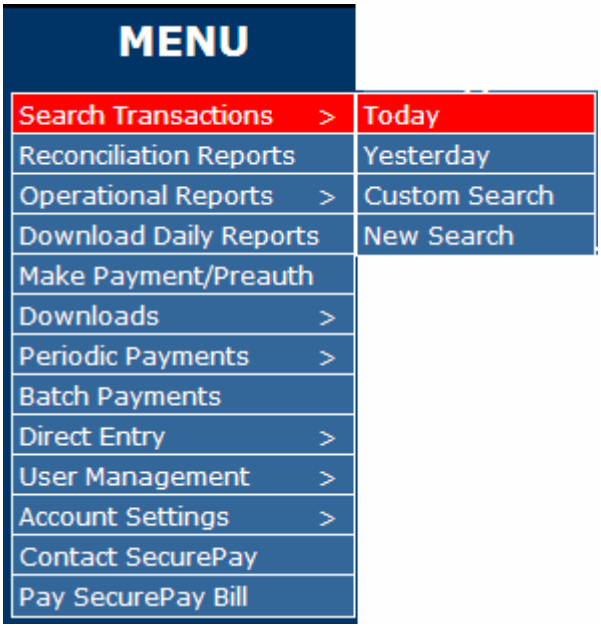
© 2008 4IPNET, INC.

▪ How does Merchant check billing transactions?

1. Go to SecurePay Merchant Login Page at https://www.securepay.com.au/merchant/ and enter **Merchant ID**, Login **User Name** and **Password**.

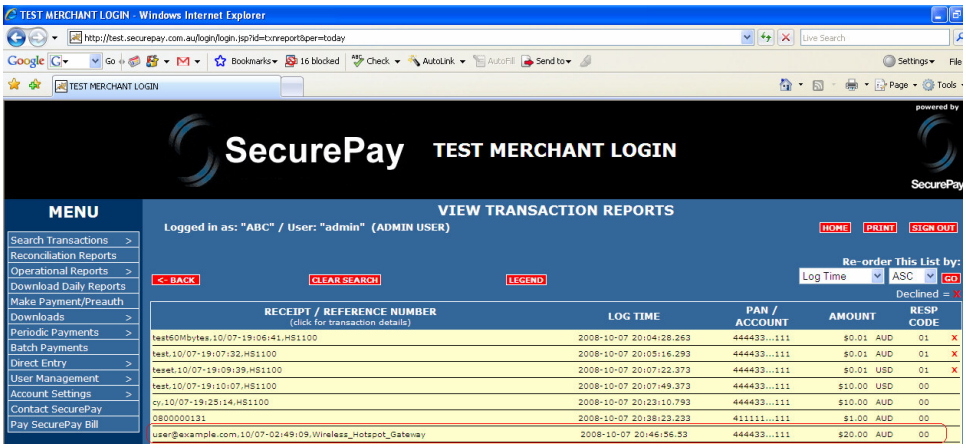


2. Click "Search Transactions" and "Today" to check today's transactions.



© 2008 4IPNET, INC.

3. Today's transaction is shown in table.

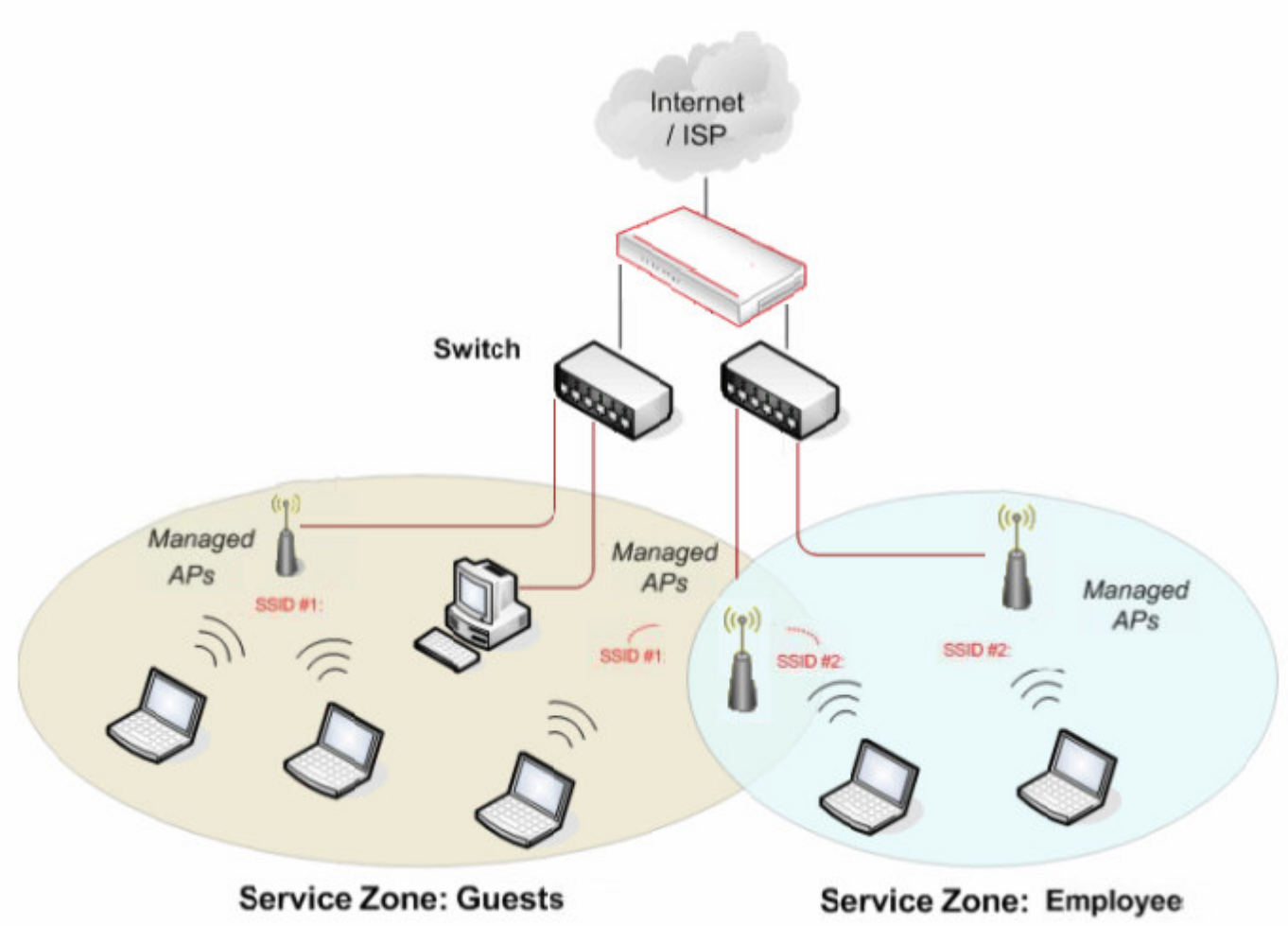


© 2008 4IPNET, INC.

Appendix D. Service Zone Deployment Example

▪ Port-Based Service Zone

In **Port-Based** mode, each LAN port can only serve traffic from one Service Zone. An example of network application diagram is shown as below: one Service Zone for **Guests** and one for **Employee**.



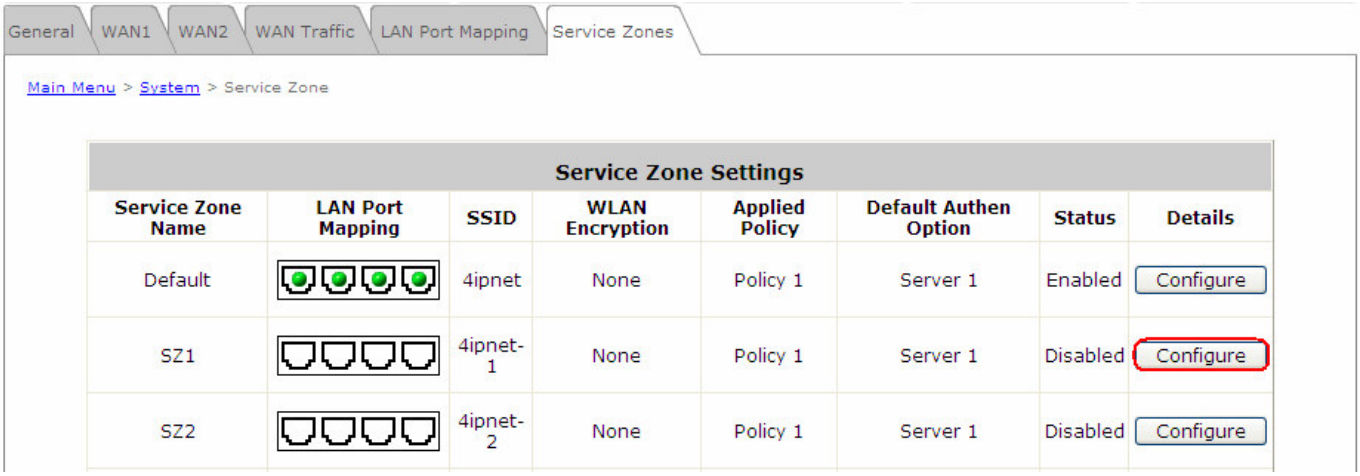
The switches deployed under WHG303 in Port-Based mode must be Layer 2 switches only.

• Configuration Steps for Port-Based Service Zones:

Step 1: Configure Service Zone 1 for Guests

Assume that **LAN1** is assigned to the **Service Zone 1** (**SZ1**) for **Guests**. Click the **System Configuration** menu and select the **Service Zones** tab. Click ***Configure*** of SZ1.

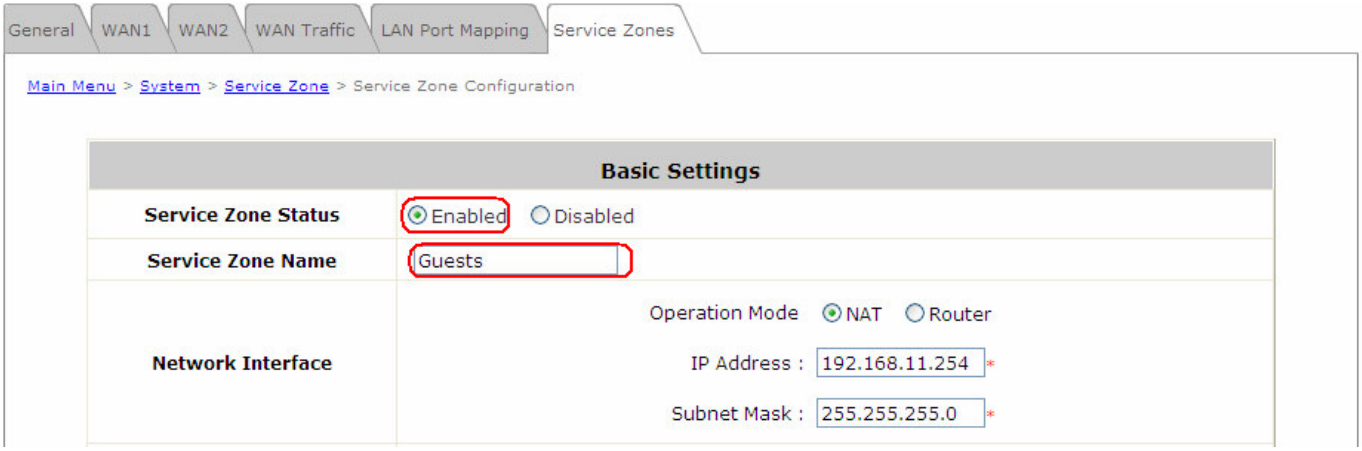
© 2008 4IPNET, INC.



Step 2: Configure Basic Settings for SZ1

Check the ***Enable*** radio button of *Service Zone Status* to activate SZ1.

Enter a name for SZ1 (e.g. **"Guests"**) in the *Service Zone Name* field.

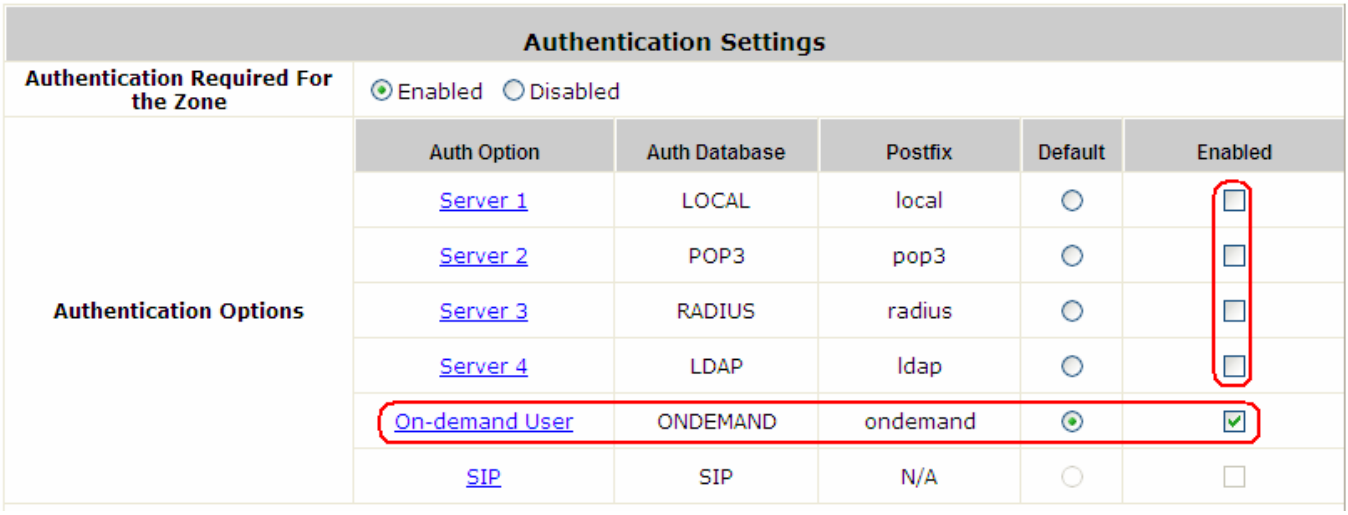


Step 3: Configure Authentication Settings for SZ1

Check the ***Enable*** radio button to enable *Authentication Required for the Zone*.

Check the ***Default*** button and ***Enabled*** box of *Guest Users* to set **ONDEMAND** authentication method as default. Disable all other authentication options. Then, click ***Apply*** to activate the settings made so far. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

© 2008 4IPNET, INC.



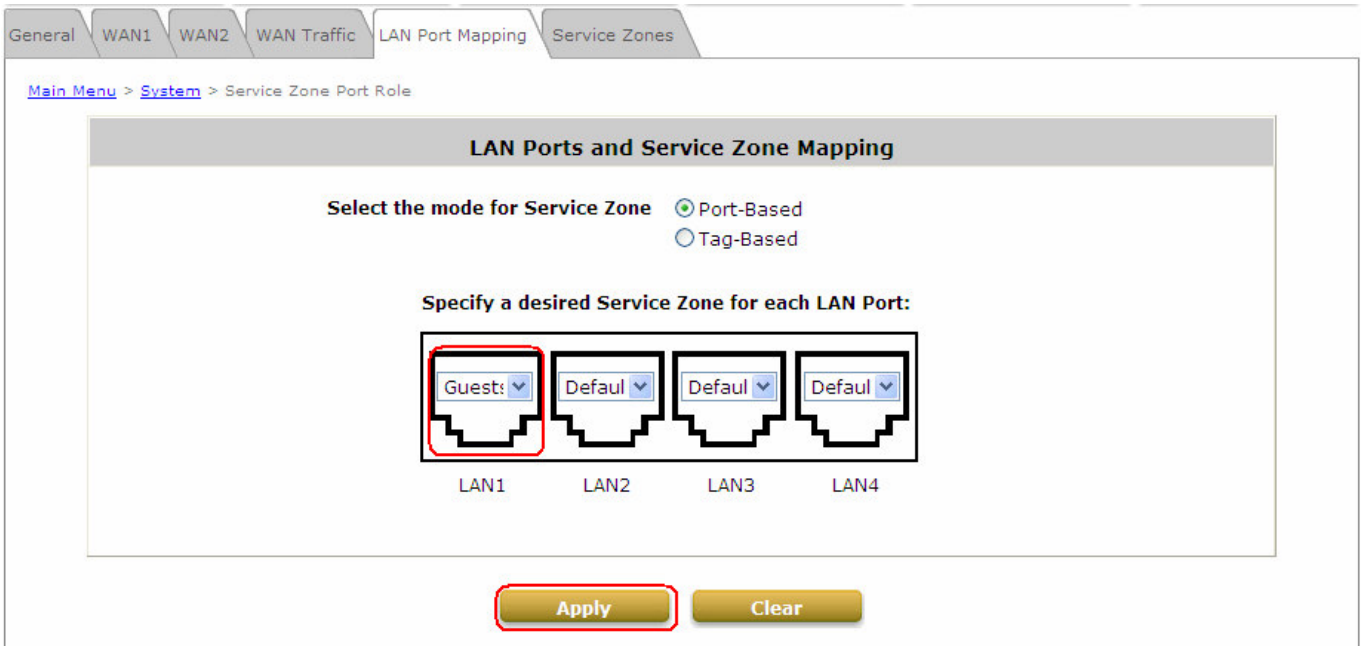
Step 4: Set Policy SZ1

Select **Policy 1** from the drop-down list box.

Click ***Apply*** to activate the settings.

Step 5: Configure LAN Port Mapping for SZ1

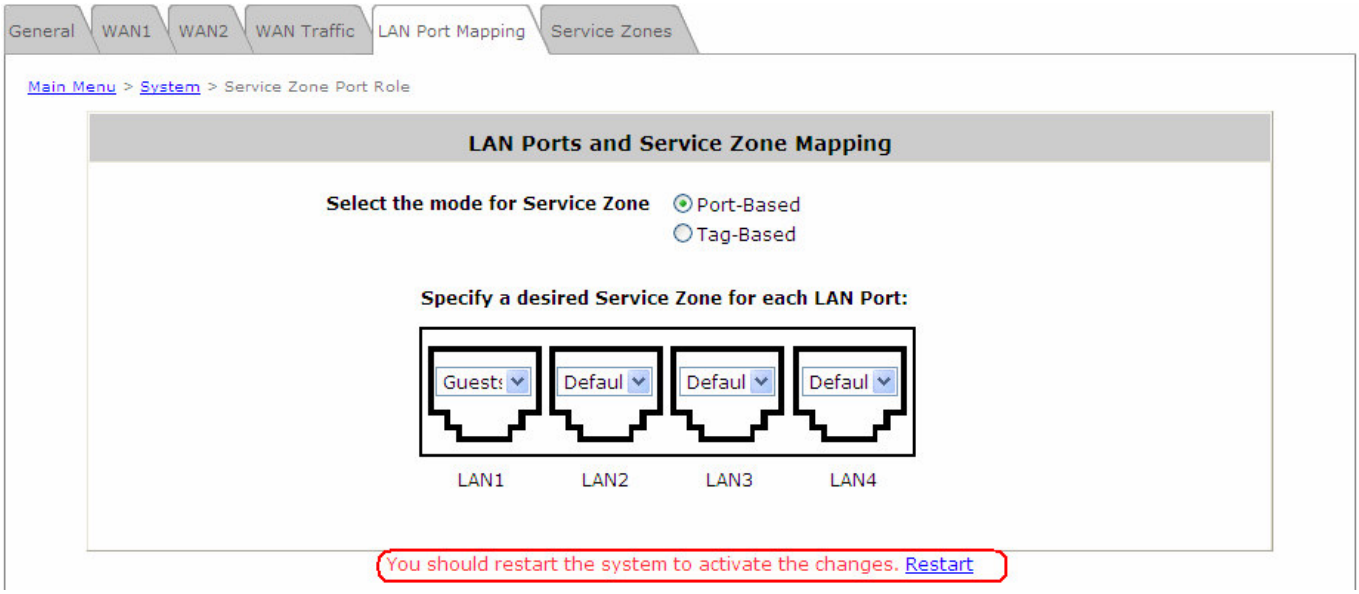
Select the **LAN Port Mapping** tab from the ***System*** menu to enter the **LAN Ports and Service Zone Mapping** page. Select ***Guests*** from the drop-down list box of LAN1. Click ***Apply*** to save the selection.



A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the

© 2008 4IPNET, INC.

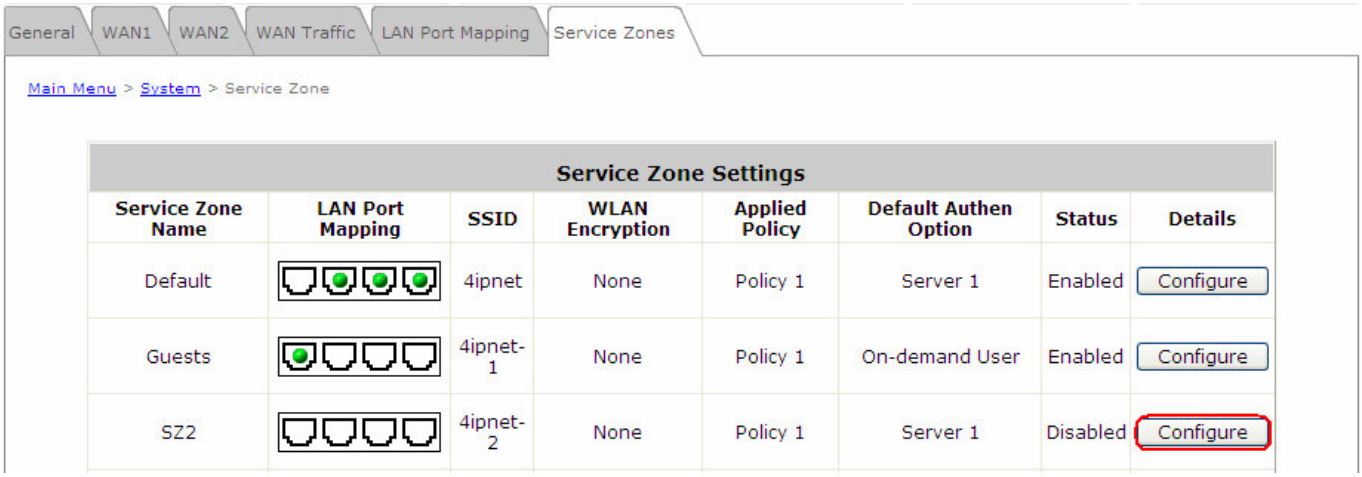
page. Do NOT restart the system until you have completed all the configuration steps.



LAN1 is now configured for **Guests**.

Step 6: Configure Service Zone 2 for Employee

Assume that **LAN2** is assigned to the **Service Zone 2** (**SZ2**) for **Employee**. Select the **Service Zones** tab and click ***Configure*** of SZ2.

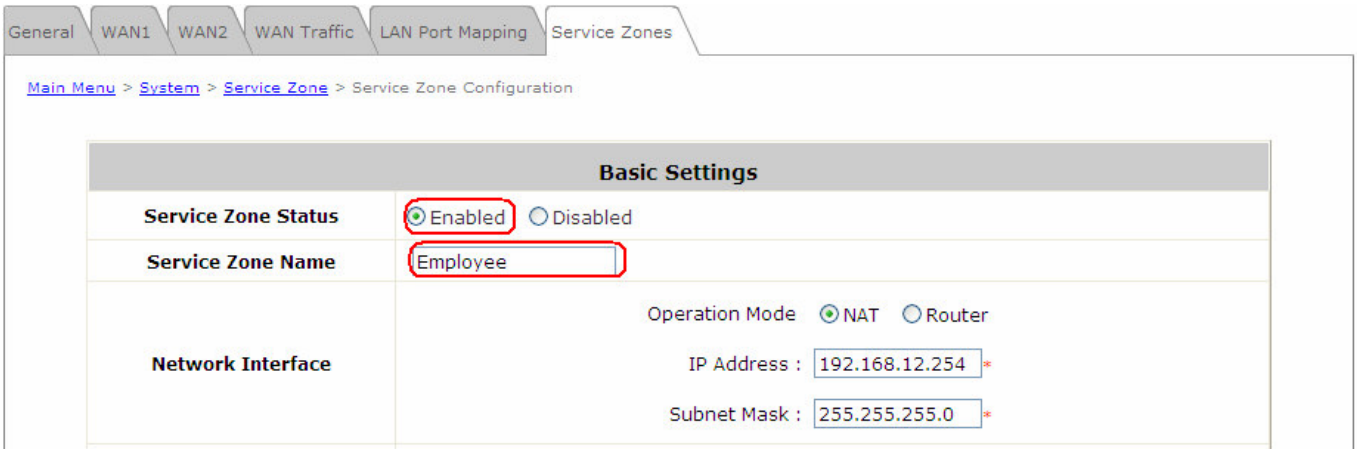


Step 7: Configure Basic Settings for SZ2

Check the ***Enable*** radio button of *Service Zone Status* to activate SZ2.

Enter a name for SZ2 (e.g. **Employee**) in the *Service Zone Name* field.

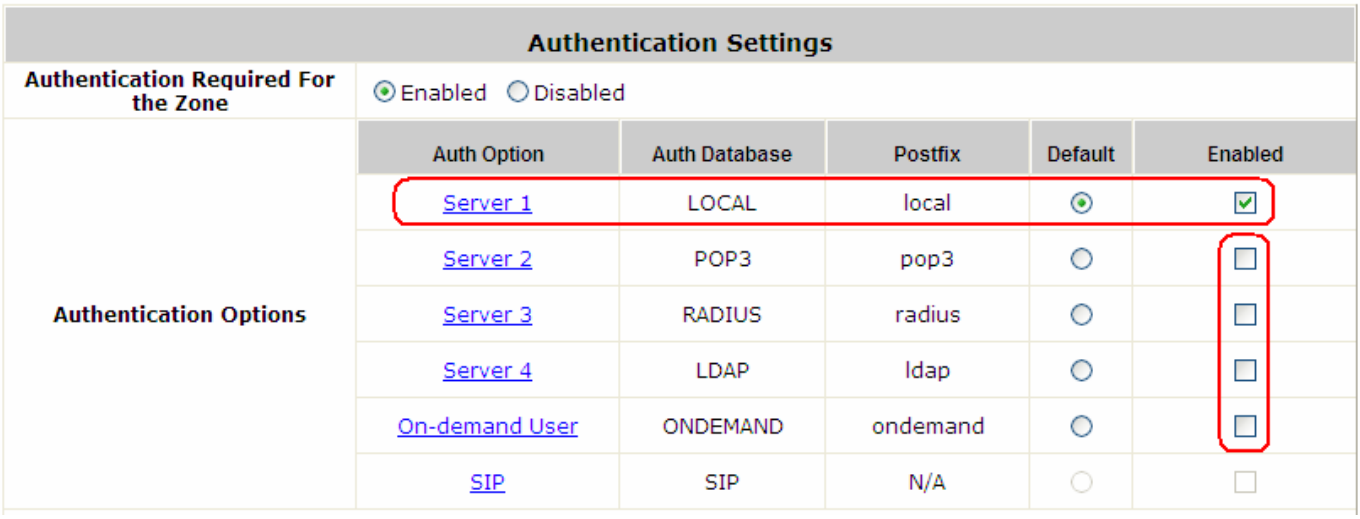
© 2008 4IPNET, INC.



Step 8: Configure Authentication Settings for SZ2

Check the ***Enable*** radio button to enable *Authentication Required for the Zone*.

Check the ***Default*** button and ***Enabled*** box of *Server 1* to set **LOCAL** authentication method as default. Disable all other authentication options. Then, click ***Apply*** to activate the settings made so far. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.



Step 9: Set Policy SZ2

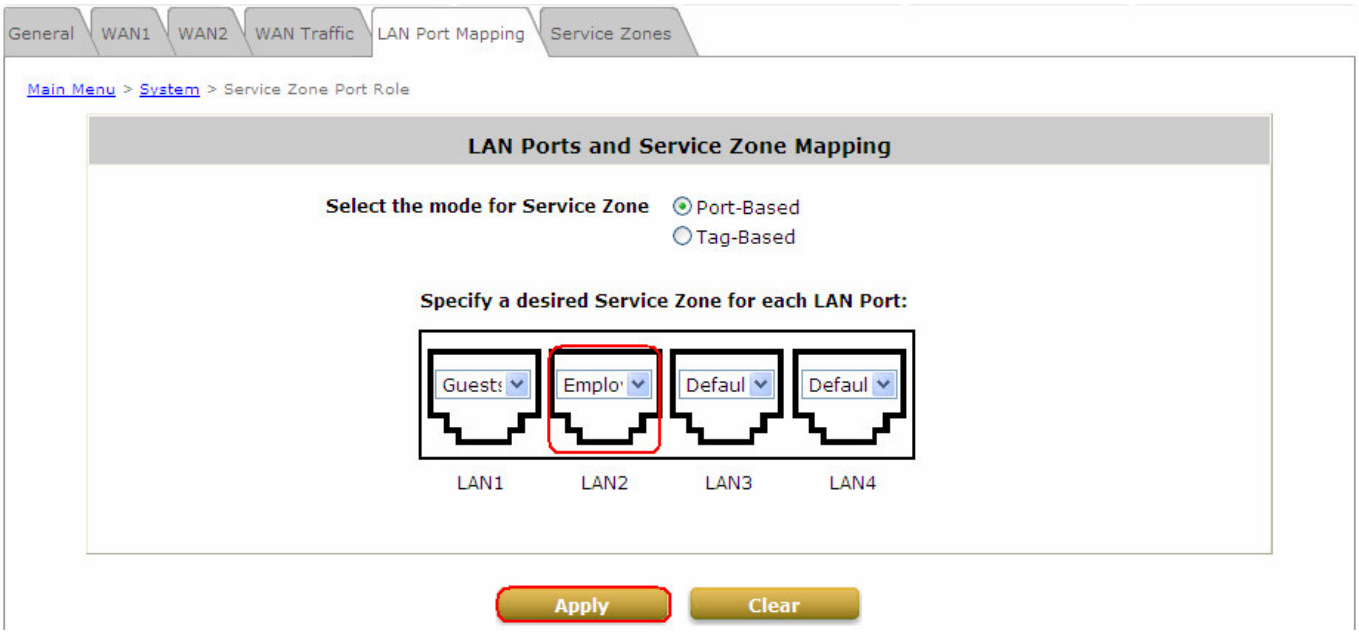
Select **Policy 1** from the drop-down list box.

Click ***Apply*** to activate the settings.

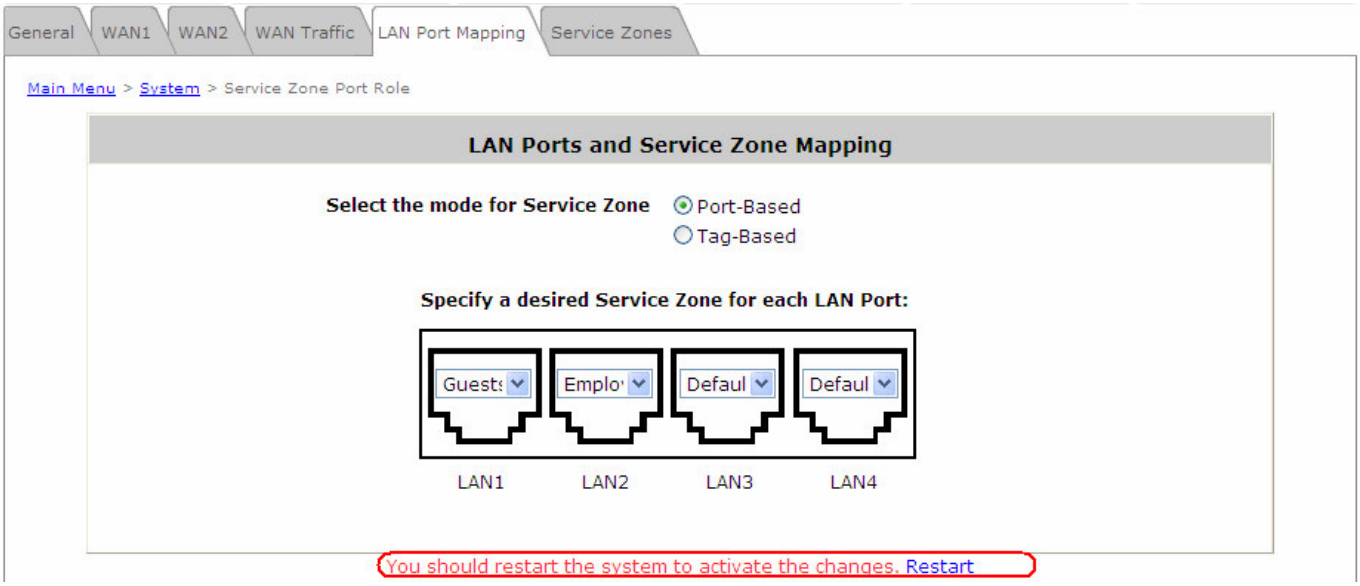
Step 10: Configure LAN Port Mapping for SZ2

© 2008 4IPNET, INC.

Select the **LAN Port Mapping** tab from the ***System*** menu to enter the **LAN Ports and Service Zone Mapping** page. Select ***Employee*** from the drop-down list box of LAN2. Click ***Apply*** to save the selection.



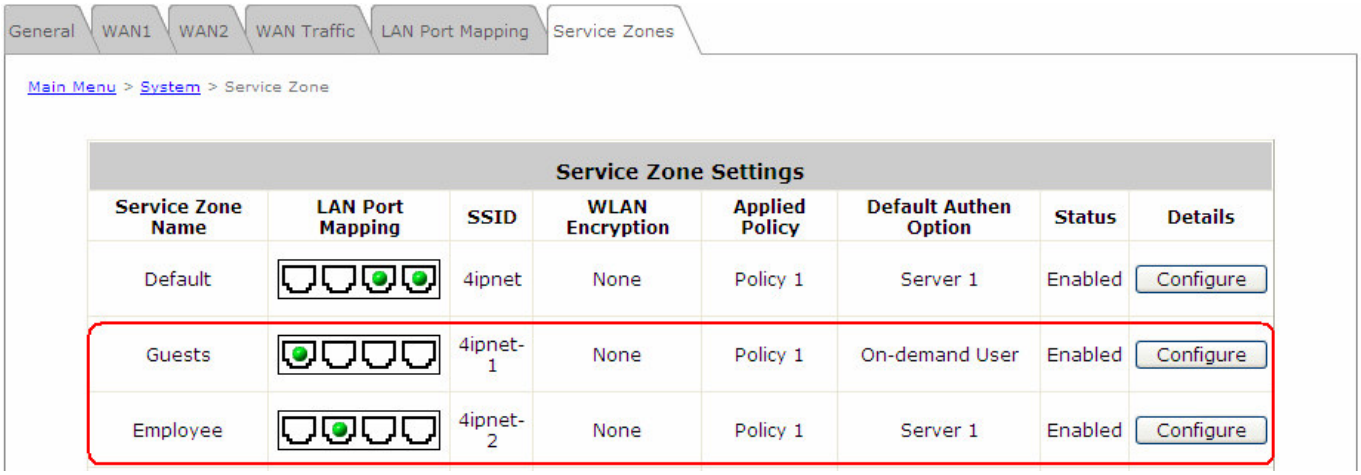
A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Click the hyperlink of **Restart** to restart the system and activate all configurations.



Please do not interrupt the system during the restarting process.

Once the settings of two Service Zones are completed, the configured result will be displayed in the **Service Zone Settings** page: **SZ1** and **SZ2** are both enabled.

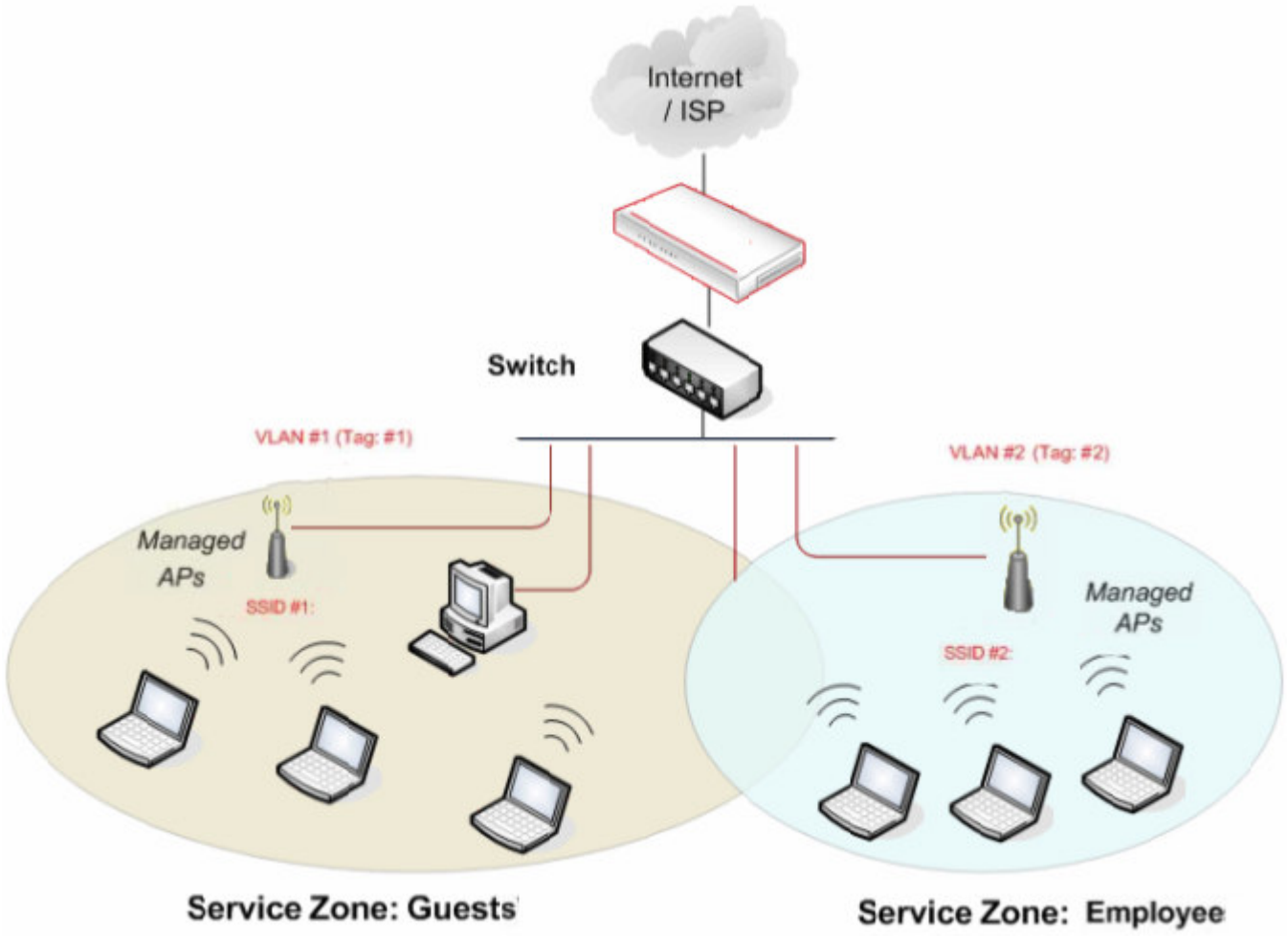
© 2008 4IPNET, INC.



© 2008 4IPNET, INC.

▪ Tag-Based Service Zone

In **Port-Based** mode, each LAN port can only serve traffic from one Service Zone. An example of network application diagram is shown as below: one Service Zone for **Guests** and one for **Employee**.



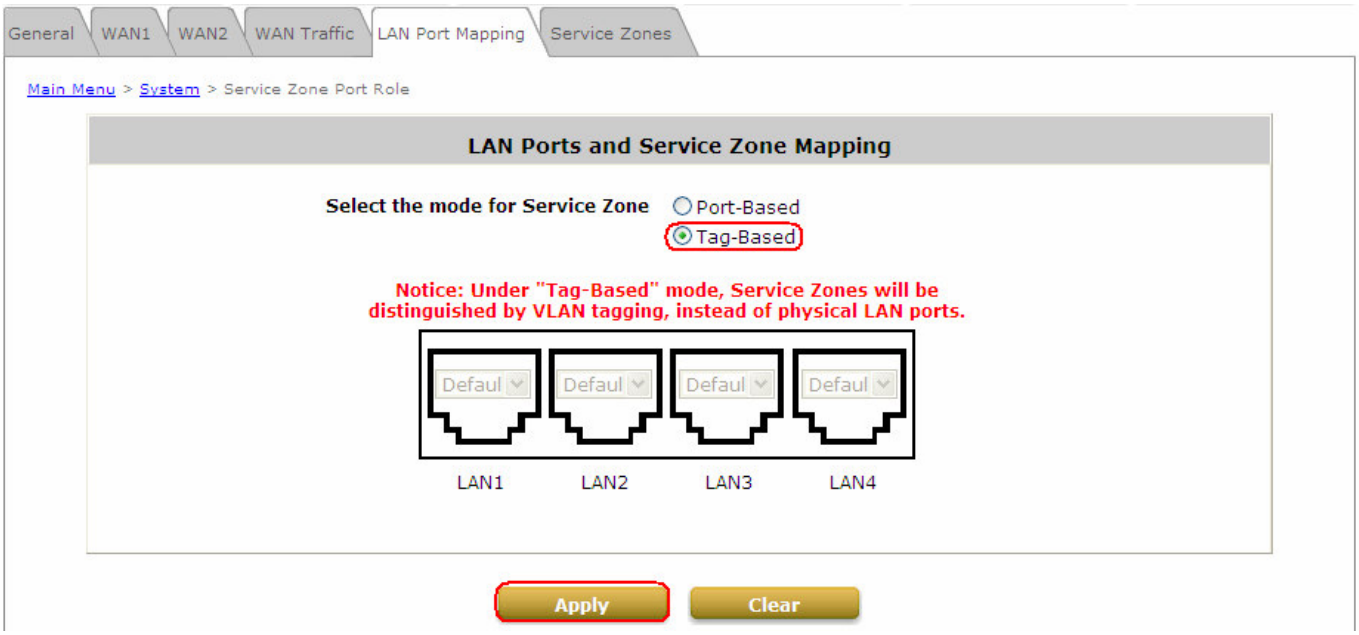
*The switch deployed under WHG303 in **Tag-Based** mode must be a **VLAN switch** only.*

• Configuration Steps for Tag-Based Service Zones:

Step 1: Set Tag-Based mode

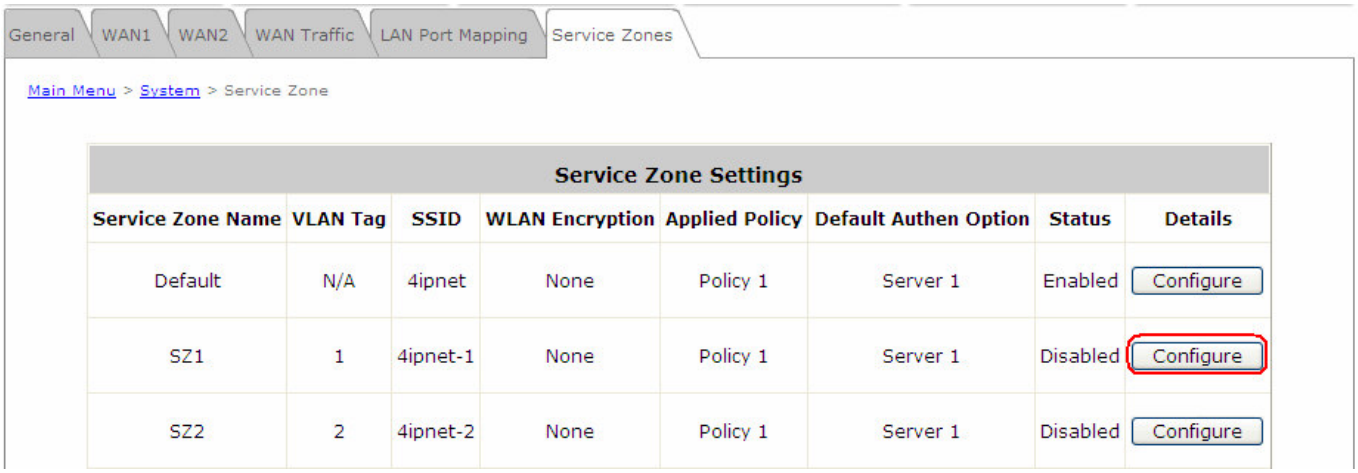
Click the **System** menu and select the **LAN Port Mapping** tab. Select ***Tag-Based*** mode and click ***Apply***. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

© 2008 4IPNET, INC.



Step 2: Configure Service Zone 1 for Guests

Select the **Service Zones** tab and click ***Configure*** of SZ1.



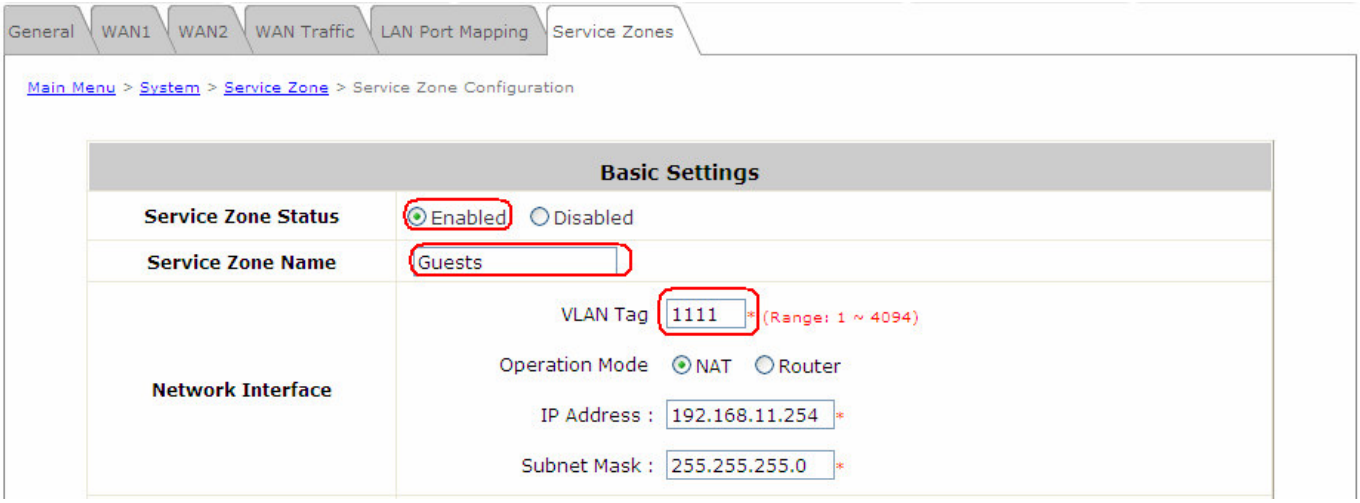
Step 3: Configure Basic Settings for SZ1

Check the ***Enable*** radio button of *Service Zone Status* to activate SZ1.

Enter a name for SZ1 (e.g. **"Guests"**) in the *Service Zone Name* field.

Enter a VLAN tag for SZ1 (e.g. **"1111"**) in the VLAN Tag field.

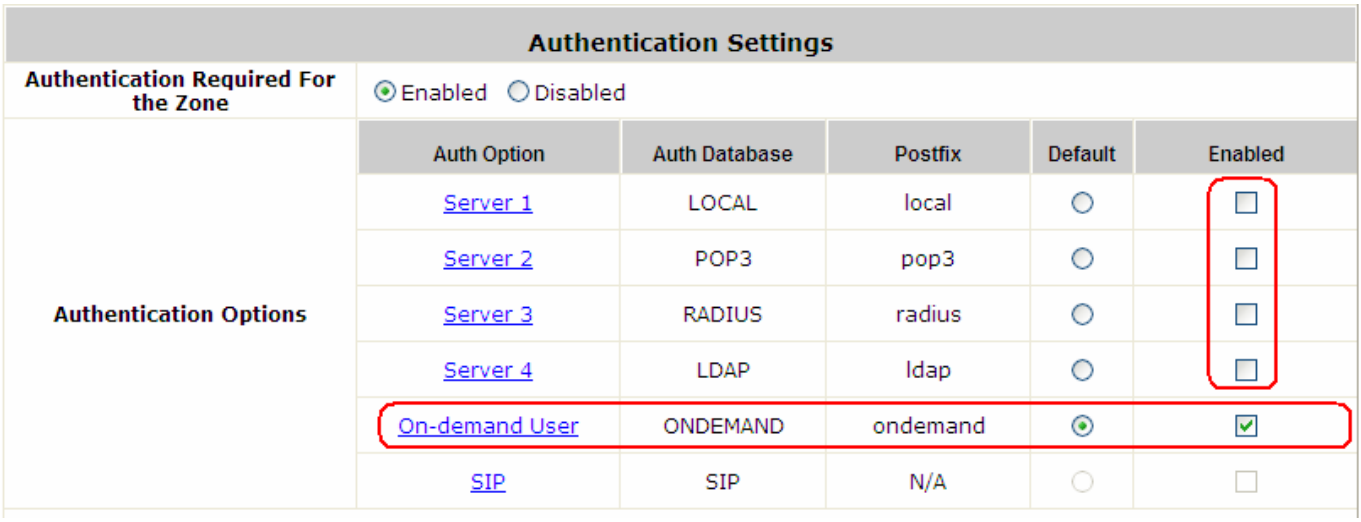
© 2008 4IPNET, INC.



Step 4: Configure Authentication Settings for SZ1

Check the ***Enable*** radio button to enable *Authentication Required for the Zone*.

Check the ***Default*** button and ***Enabled*** box of *Guest Users* to set **ONDEMAND** authentication method as default. Disable all other authentication options. Then, click ***Apply*** to activate the settings made so far. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.



Step 5: Set Policy SZ1

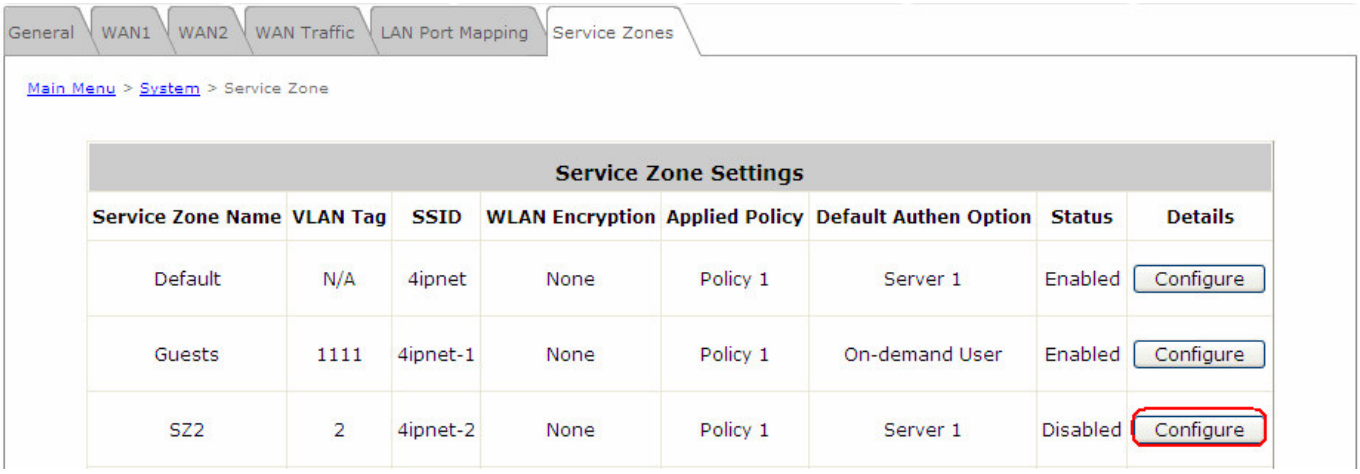
Select **Policy 1** from the drop-down list box.

Click ***Apply*** to activate the settings. Click ***Apply*** to activate the settings made so far. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

© 2008 4IPNET, INC.

Step 6: Configure Service Zone 2 for Employee

Assume that **LAN2** is assigned to the **Service Zone 2** (**SZ2**) for **Employee**. Select the **Service Zones** tab and click ***Configure*** of SZ2.

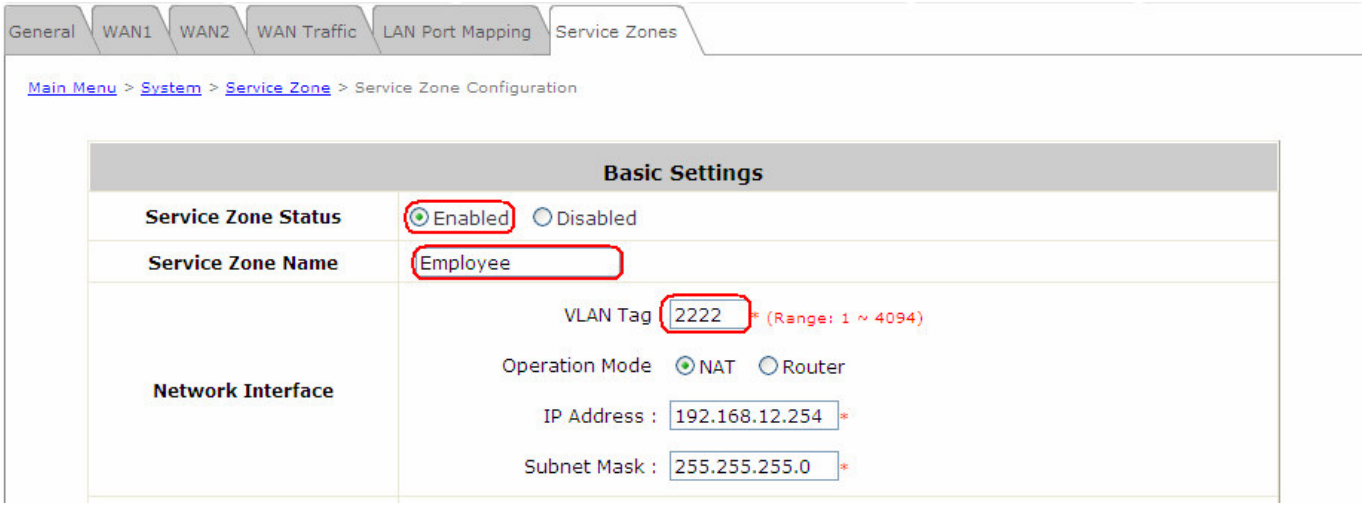


Step 7: Configure Basic Settings for SZ2

Check the ***Enable*** radio button of *Service Zone Status* to activate SZ2.

Enter a name for SZ2 (e.g. **Employee**) in the *Service Zone Name* field.

Enter a VLAN tag for SZ2 (e.g. **"2222"**) in the *VLAN Tag* field.



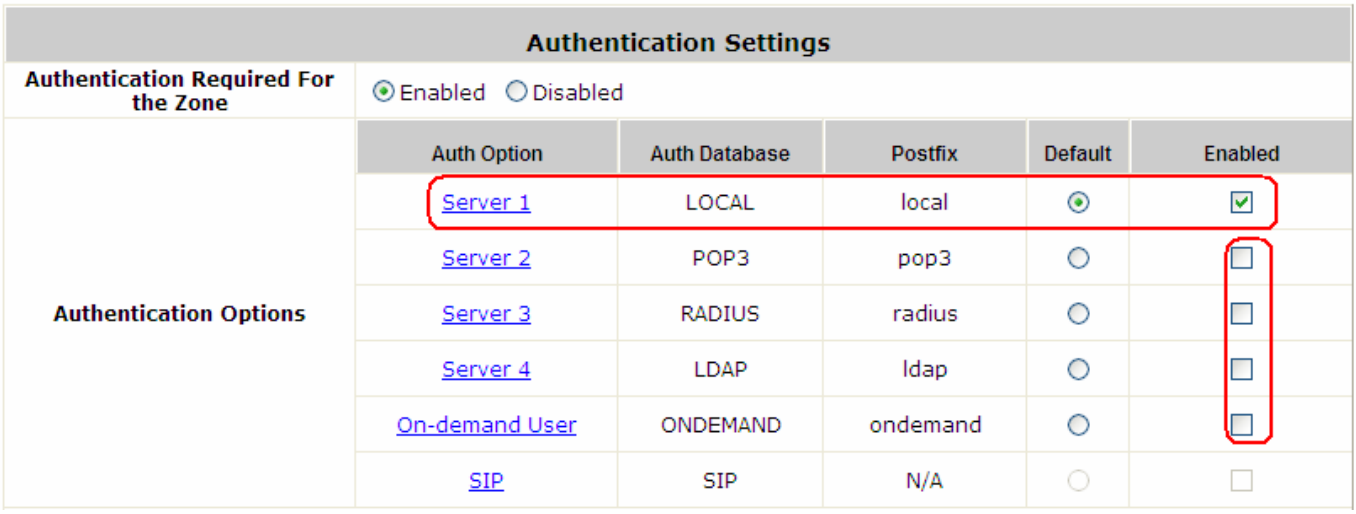
Step 8: Configure Authentication Settings for SZ2

Check the ***Enable*** radio button to enable *Authentication Required for the Zone*.

Check the ***Default*** button and ***Enabled*** box of *Server 1* to set **LOCAL** authentication method as default. Disable all

© 2008 4IPNET, INC.

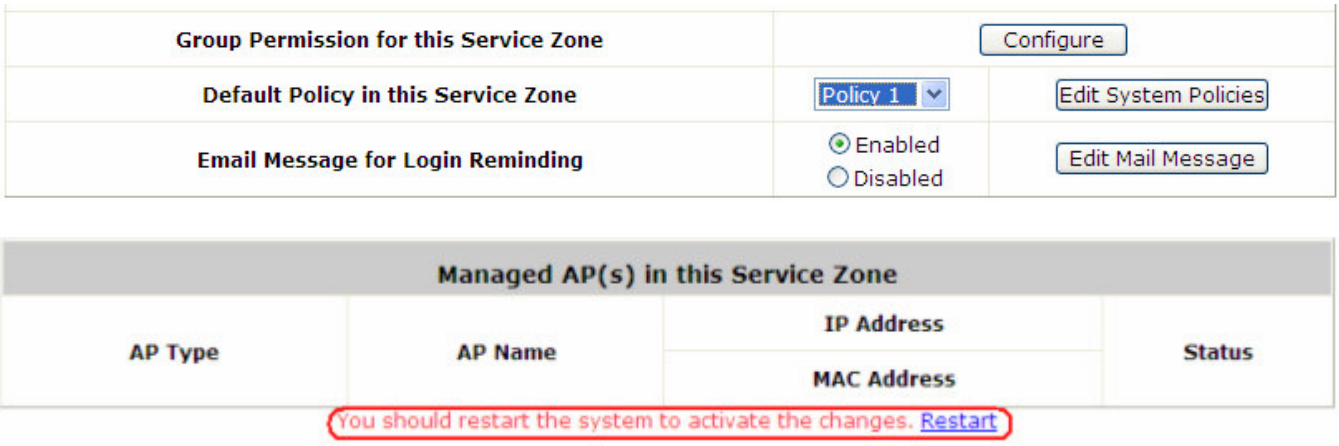
other authentication options. Then, click ***Apply*** to activate the settings made so far. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.



Step 9: Set Policy SZ2

Select **Policy 1** from the drop-down list box.

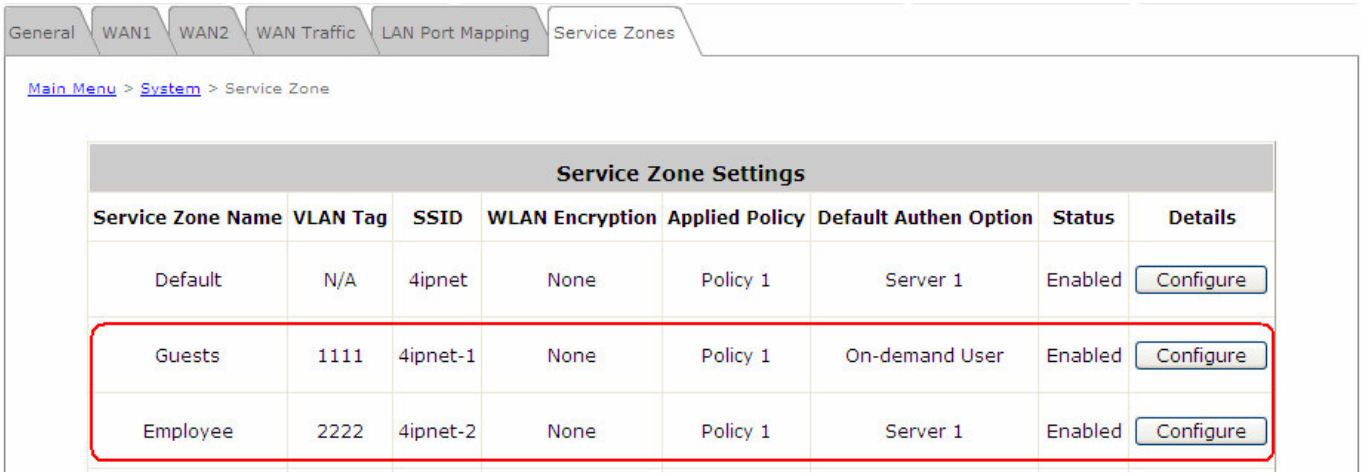
Click ***Apply*** to activate the settings. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.



Please do not interrupt the system during the restarting process.

Once the settings of two Service Zones are completed, the configured result will be displayed in the **Service Zone Settings** page: **SZ1** and **SZ2** are both enabled.

© 2008 4IPNET, INC.



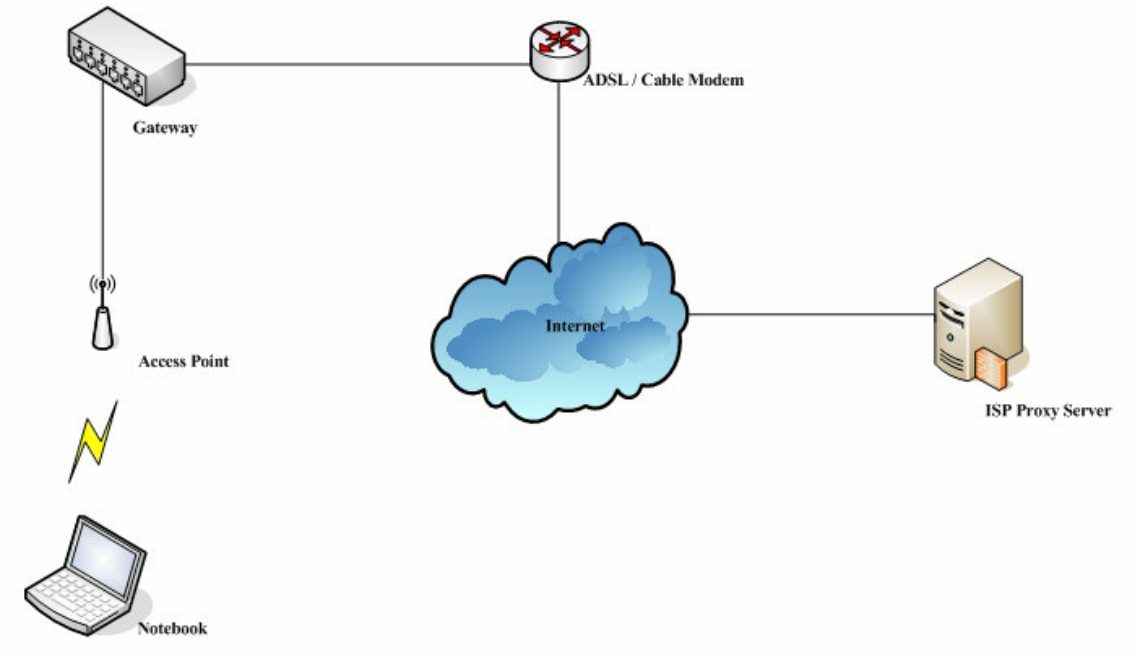
© 2008 4IPNET, INC.

Appendix E. Proxy Setting

Basically, a proxy server can help clients access the network resources more quickly. This section presents basic examples for configuring the proxy server settings of WHG303.

▪ Using Internet Proxy Server

The first scenario is that a proxy server is placed outside the LAN environment or in the Internet. For example, the following diagram shows that a proxy server of an ISP will be used.

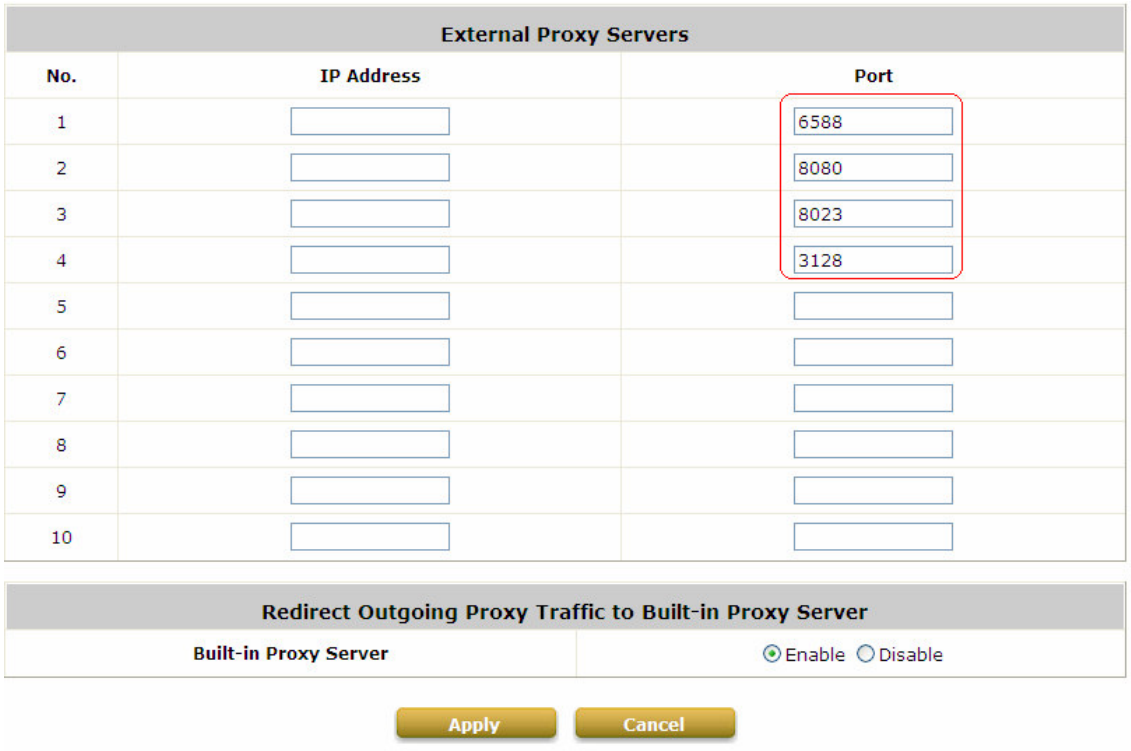


© 2008 4IPNET, INC.

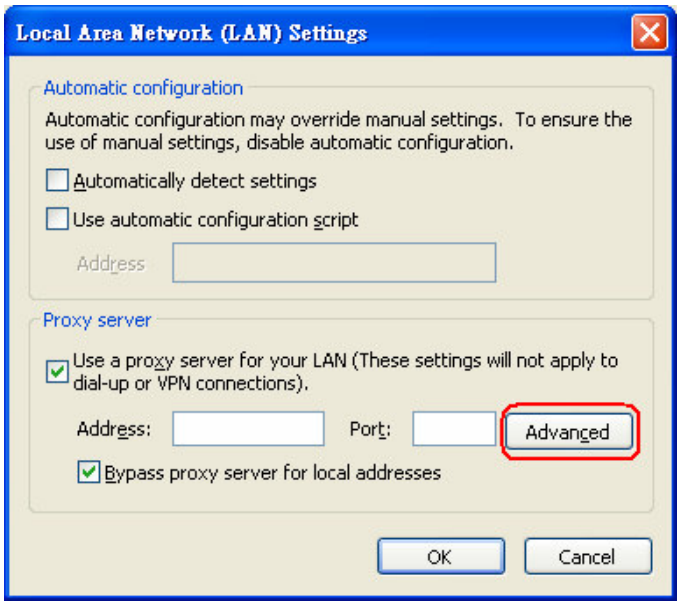
Follow the following steps to complete the proxy configuration:

Step 1. Log into the system by using the ***admin*** account.

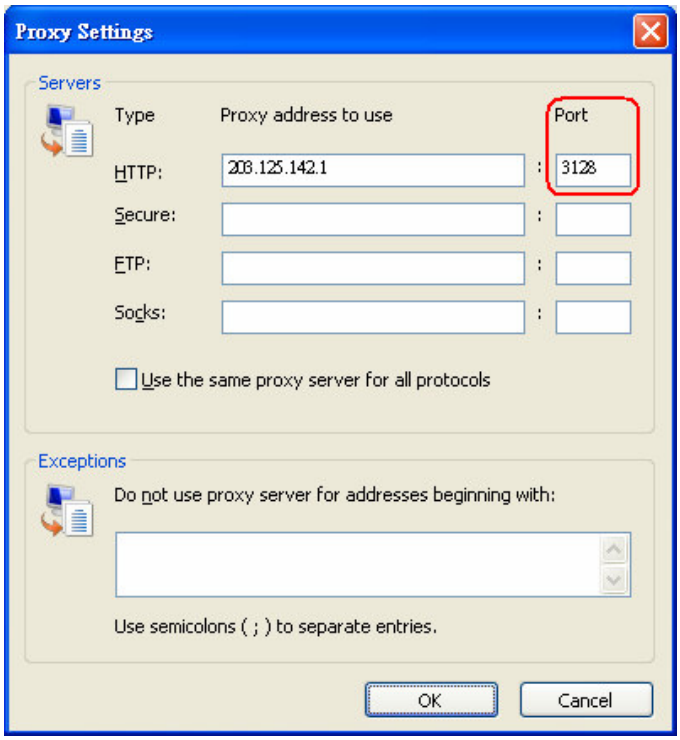
Step 2. ***Network*** >> ***Proxy Server*** >> ***External Proxy Servers*** page. Add the IP address (leaving it blank means any IP address) and port number of the proxy servers into ***External Proxy Servers*** setting. Enable the ***Built-in Proxy Server***. Click ***Apply*** to save the settings.



Step 3. Make sure that the proxy server settings match with at least one of the proxy server setting of the system – for example, in this case, 203.125.142.1:**3128** matches with blank:**3128**.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
Advanced
Bypass proxy server for local addresses
OK
Cancel

© 2008 4IPNET, INC.

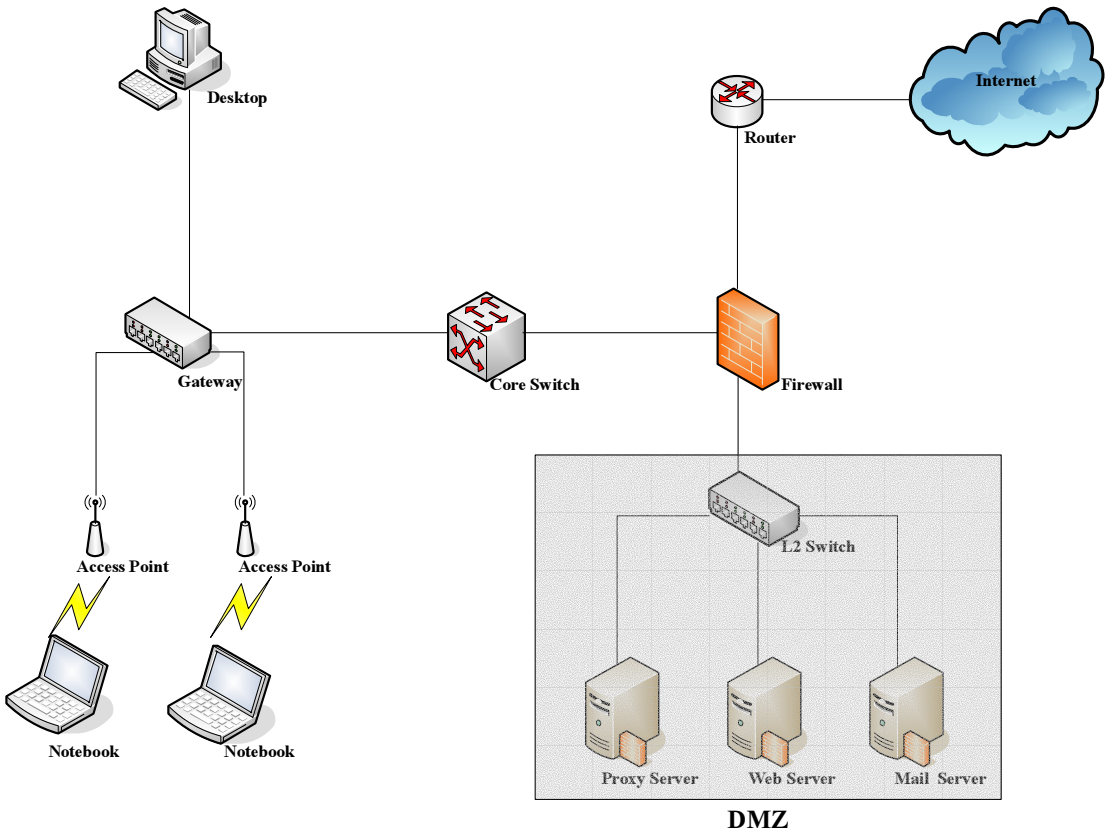


1. *It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*
2. *What the **Built-in Proxy Server** is enabled, all the outgoing proxy traffic will be automatically redirected to the built-in proxy server.*

© 2008 4IPNET, INC.

▪ Using Extranet Proxy Server

The second scenario is that a proxy server is placed in the Extranet (such as DMZ), which all users from the Intranet or the Internet are able to access. For example, the following diagram shows that a proxy server of an organization in the DMZ will be used.



A special scenario is that a proxy server is placed in a zone like Intranet – where users can reach each other without going through the system. In this case, whenever any one of users in the Intranet has been authenticated and connects to the network via the proxy server, other users using the same proxy setting in their browsers will be able to access the network without any authentication. Therefore, to stop the risk, it is strongly recommended to put all proxy servers outside the Intranet.

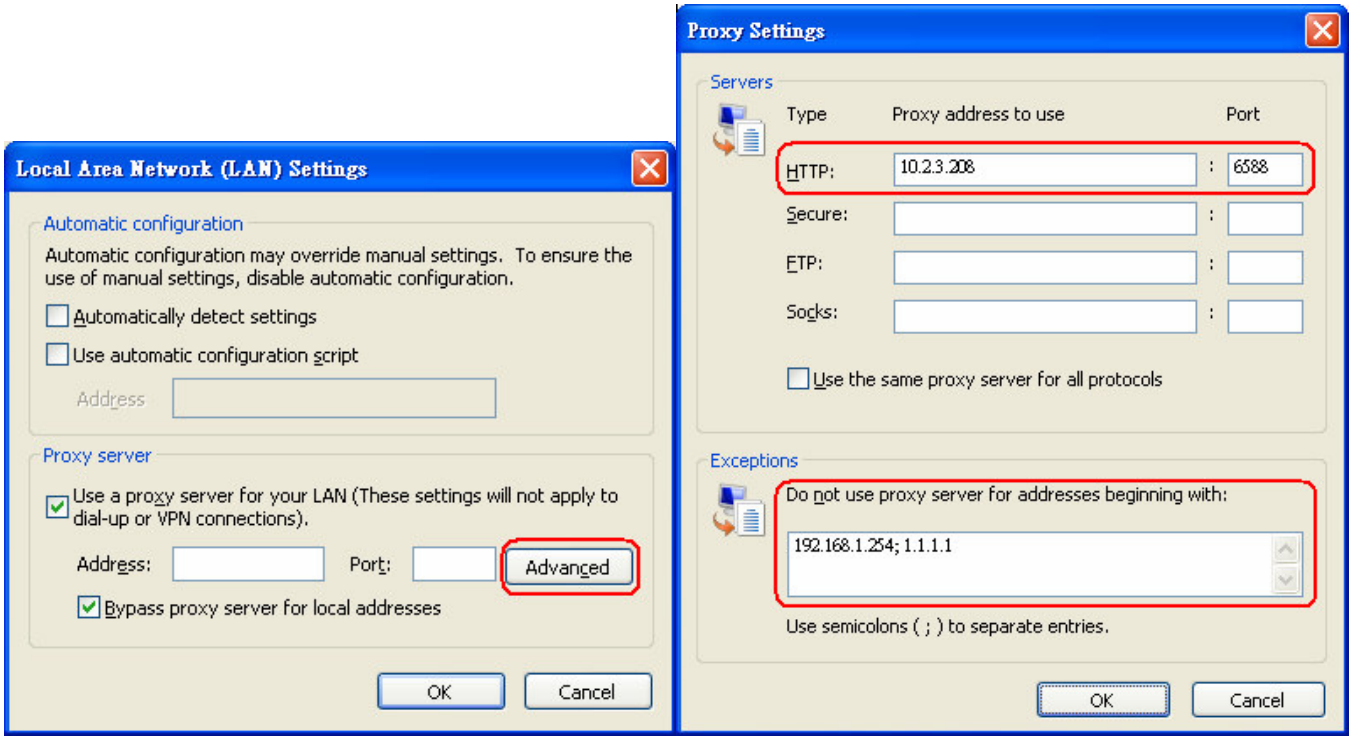
Follow the following steps to complete the proxy configuration:

Step 1. Log into the system by using the ***admin*** account.

Step 2. ***Network*** >> ***Proxy Server*** >> ***External Proxy Servers*** page. Add the IP address and port number of the proxy server into External Proxy Servers setting. Click ***Apply*** to save the settings.

Step 3. Make sure that clients use the same proxy server settings. Please also configure appropriate exceptions if there is any traffic which is not needed to go through proxy server – for example, there is no need to use proxy server for the Default Gateway (192.168.1.254).

© 2008 4IPNET, INC.



It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will shown an error page in the browser.

© 2008 4IPNET, INC.

Appendix F. Session Limit and Session Log

▪ Session Limit

To prevent ill-behaved clients or malicious software from using up the system's connection resources, the administrator can restrict the number of concurrent sessions that a user can establish.

- The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones.
- When the number of a user's sessions reaches the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350 and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a Syslog server.
- Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

▪ Session Log

The system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to a specified Syslog Server, Email Box or FTP Server based on pre-defined interval time.

- The description of the fields of a session log record is shown as below:

Field	Description
Date and Time	The date and time that the session is established
Session Type	[New]: This is a newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user. When it shows "N.A.", it indicates that the user or device does not need to log in with a username, for example, the user or device is on a non-authenticated port or on the privileged MAC/IP list. Change the account name accordingly, if the name is not identifiable in the record. ⏩ **Note:** Only 31 characters are allowed for the combination of Session Type plus Username.
Protocol	The communication protocol of session: TCP or UDP
MAC	The MAC address of the user's computer or device
SIP	The source IP address of the user's computer or device
SPort	The source port number of the user's computer or device
DIP	The destination IP address of the user's computer or device
DPort	The destination port number of the user's computer or device

© 2008 4IPNET, INC.

- An example of session log data is shown as below:

```
31 Aug 12:35:05 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1626 DIP=203.125.164.132 DPort=80
31 Aug 12:35:05 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1627 DIP=203.125.164.132 DPort=80
31 Aug 12:35:06 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1628 DIP=203.125.164.142 DPort=80
31 Aug 12:35:06 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1629 DIP=203.125.164.142 DPort=80
31 Aug 12:35:07 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1630 DIP=67.18.163.154 DPort=80
31 Aug 12:35:09 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1631 DIP=202.43.195.52 DPort=80
31 Aug 12:35:10 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1632 DIP=203.84.196.242 DPort=80
```


© 2008 4IPNET, INC.

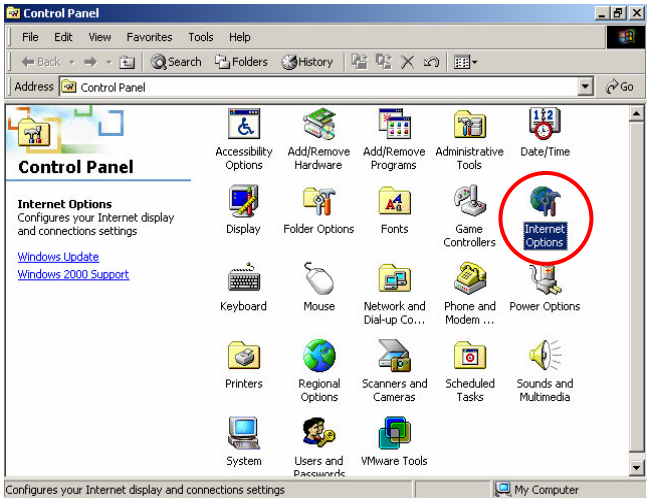
Appendix G. Network Configuration on PC & User Login

▪ Network Configuration on PC

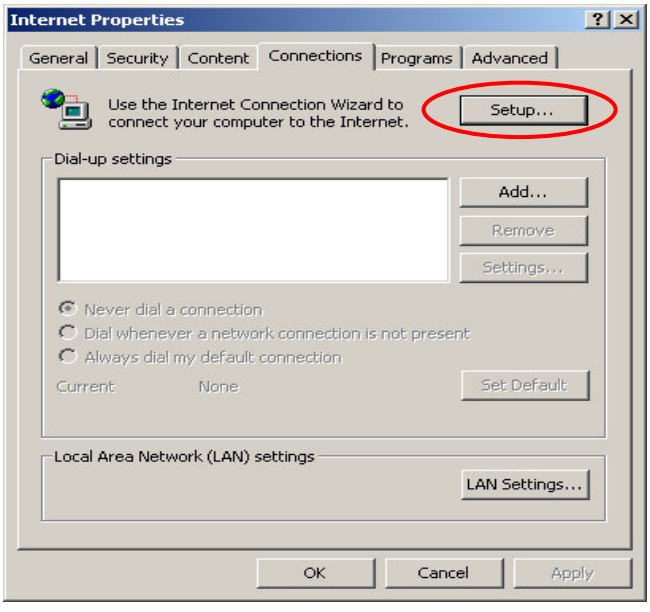
After 4ipnet WHG303 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**
  - **Windows 9x/2000**

1) Choose **Start** >> **Control Panel** >> **Internet Options**.

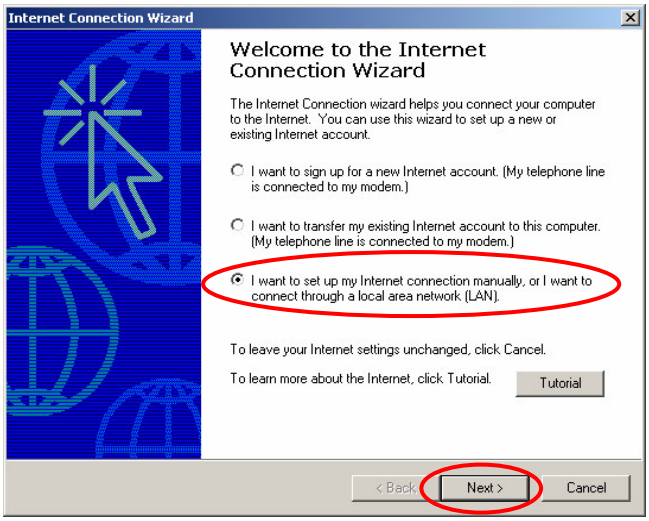


2) Choose the **Connections** tab, and then click ***Setup***.

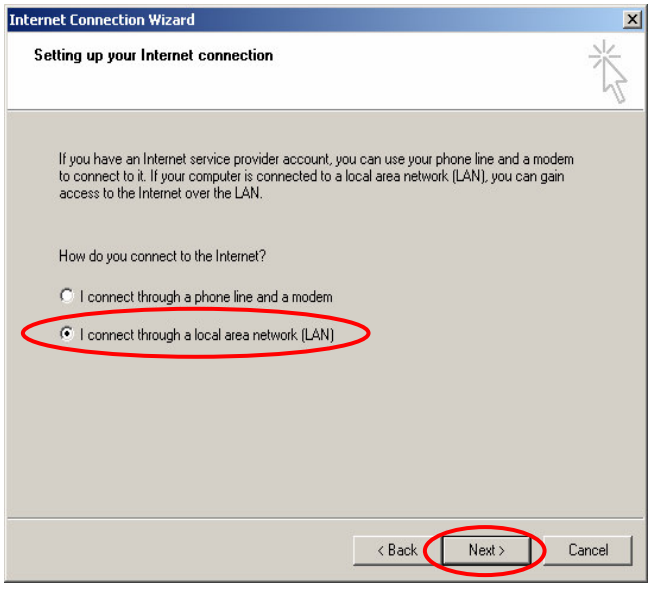


© 2008 4IPNET, INC.

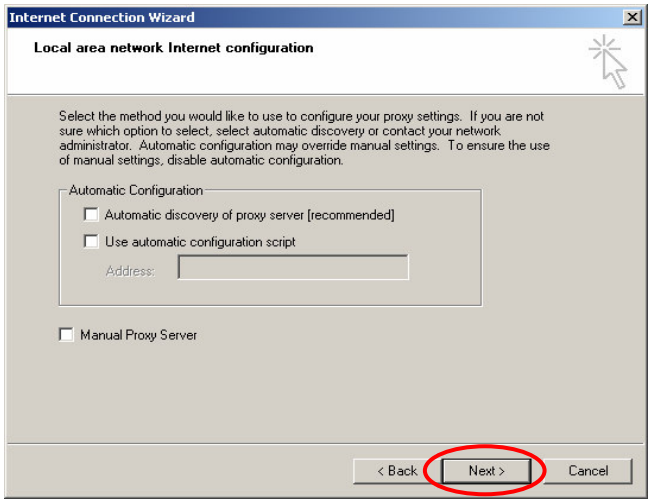
3) Choose **"I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)"**, and then click ***Next***.


Internet Connection Wizard
Welcome to the Internet Connection Wizard
The Internet Connection wizard helps you connect your computer to the Internet. You can use this wizard to set up a new or existing Internet account.
I want to sign up for a new Internet account. (My telephone line is connected to my modem.)
I want to transfer my existing Internet account to this computer. (My telephone line is connected to my modem.)
I want to set up my Internet connection manually, or I want to connect through a local area network (LAN).
To leave your Internet settings unchanged, click Cancel.
To learn more about the Internet, click Tutorial.
Tutorial
< Back
Next >
Cancel

4) Choose **"I connect through a local area network (LAN)"** and then click ***Next***.

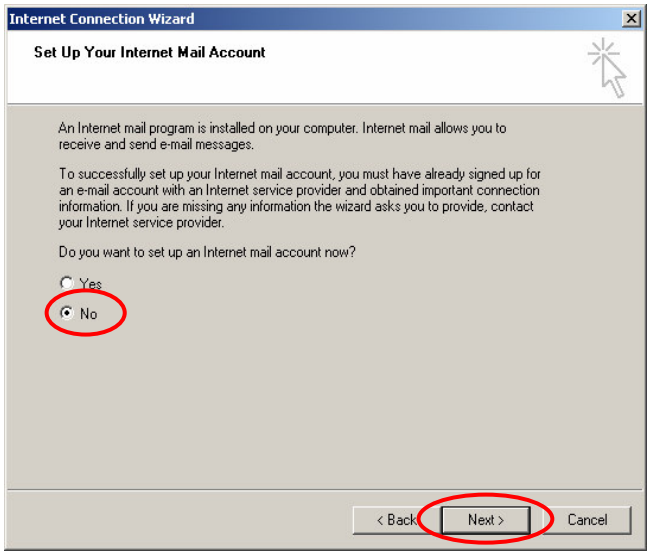

Internet Connection Wizard
Setting up your Internet connection
If you have an Internet service provider account, you can use your phone line and a modem to connect to it. If your computer is connected to a local area network (LAN), you can gain access to the Internet over the LAN.
How do you connect to the Internet?
I connect through a phone line and a modem
I connect through a local area network (LAN)
< Back
Next >
Cancel

5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click ***Next***.

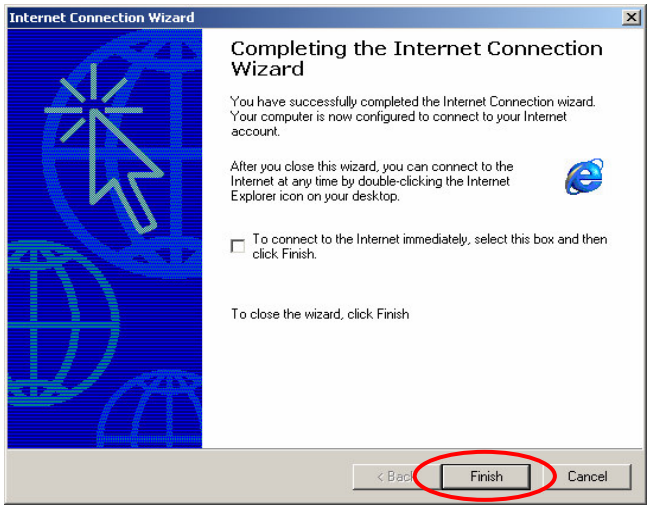

Internet Connection Wizard
Local area network Internet configuration
Select the method you would like to use to configure your proxy settings. If you are not sure which option to select, select automatic discovery or contact your network administrator. Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatic Configuration
Automatic discovery of proxy server [recommended]
Use automatic configuration script
Address:
Manual Proxy Server
< Back
Next >
Cancel

© 2008 4IPNET, INC.

6) Choose **"No"** and then click ***Next***.

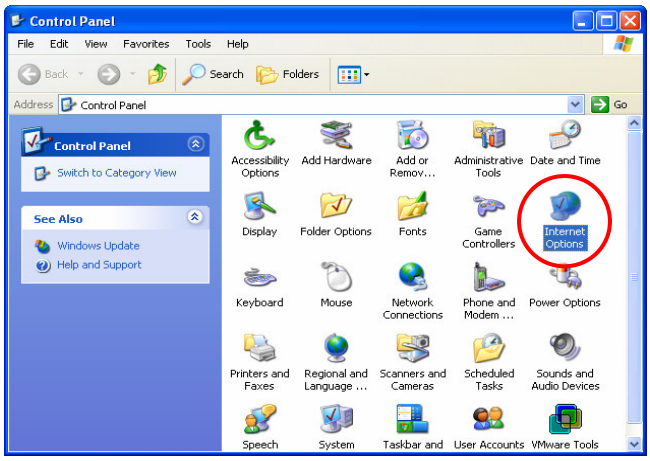

Internet Connection Wizard
Set Up Your Internet Mail Account
An Internet mail program is installed on your computer. Internet mail allows you to receive and send e-mail messages.
To successfully set up your Internet mail account, you must have already signed up for an e-mail account with an Internet service provider and obtained important connection information. If you are missing any information the wizard asks you to provide, contact your Internet service provider.
Do you want to set up an Internet mail account now?
Yes
No
< Back
Next >
Cancel

7) Finally, click ***Finish*** to exit the **Internet Connection Wizard**. Now, the set up is completed.


Internet Connection Wizard
Completing the Internet Connection Wizard
You have successfully completed the Internet Connection wizard. Your computer is now configured to connect to your Internet account.
After you close this wizard, you can connect to the Internet at any time by double-clicking the Internet Explorer icon on your desktop.
To connect to the Internet immediately, select this box and then click Finish.
To close the wizard, click Finish
< Back
Finish
Cancel

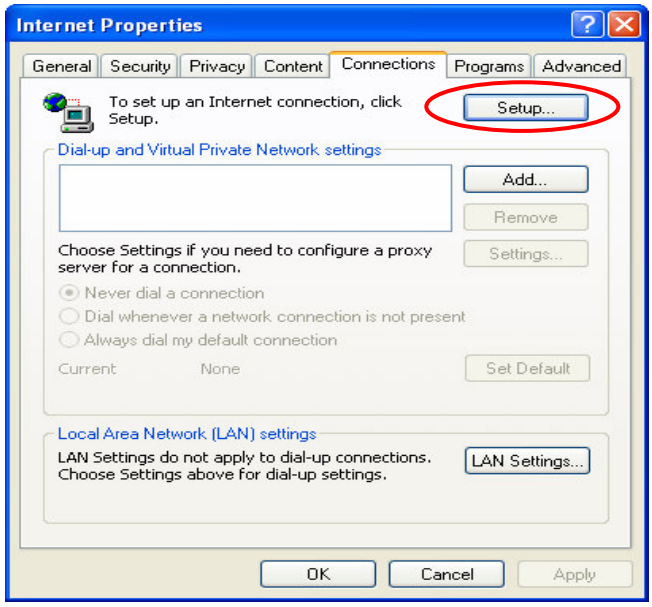
- **Windows XP**

1) Choose **Start** >> **Control Panel** >> **Internet Option**.



© 2008 4IPNET, INC.

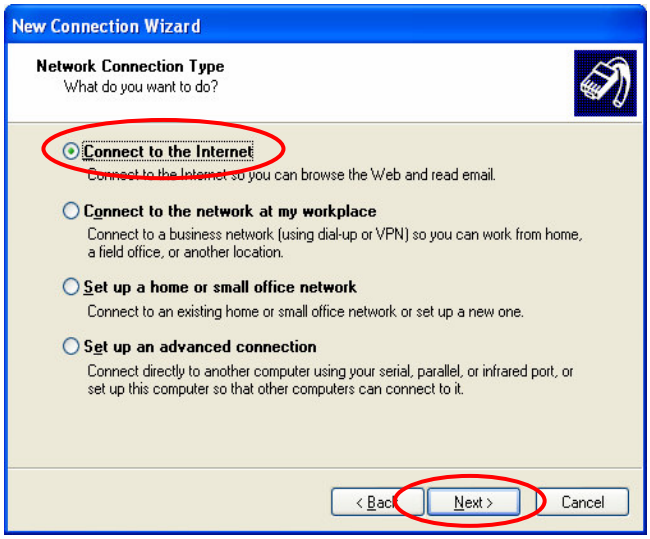
2) Choose the **Connections** tab, and then click ***Setup***.



3) When the **Welcome to the New Connection Wizard** window appears, click ***Next***.

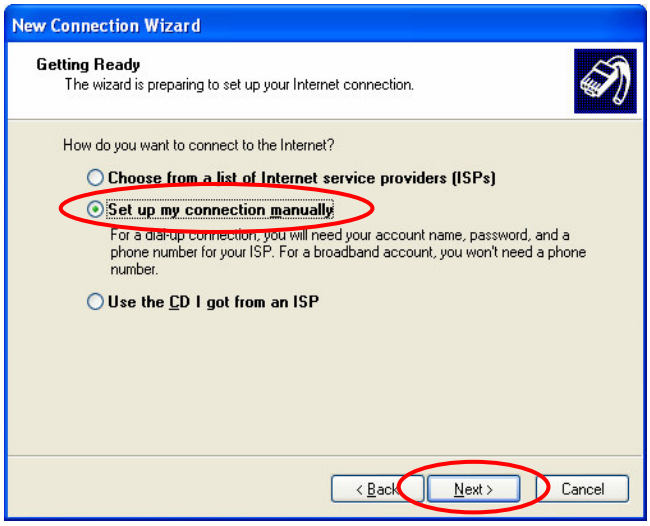
New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
Connect to the Internet.
Connect to a private network, such as your workplace network.
Set up a home or small office network.
To continue, click Next.
< Back
Next >
Cancel

4) Choose **"Connect to the Internet"** and then click ***Next***.

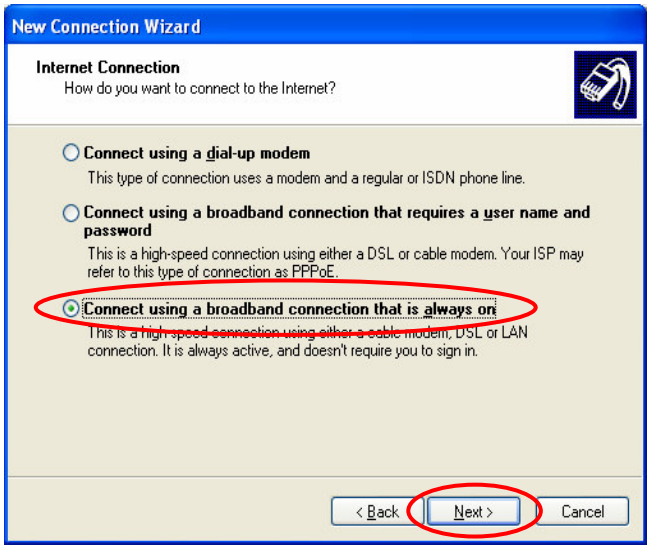

New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

© 2008 4IPNET, INC.

5) Choose **"Set up my connection manually"** and then click ***Next***.


New Connection Wizard
Getting Ready
The wizard is preparing to set up your Internet connection.
How do you want to connect to the Internet?
Choose from a list of Internet service providers (ISPs)
Set up my connection manually
For a dial-up connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number.
Use the CD I got from an ISP
< Back
Next >
Cancel

6) Choose **"Connect using a broadband connection that is always on"** and then click ***Next***.


New Connection Wizard
Internet Connection
How do you want to connect to the Internet?
Connect using a dial-up modem
This type of connection uses a modem and a regular or ISDN phone line.
Connect using a broadband connection that requires a user name and password
This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.
Connect using a broadband connection that is always on
This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.
< Back
Next >
Cancel

7) Finally, click ***Finish*** to exit the **Connection Wizard**. Now, the setup is completed.

New Connection Wizard
Completing the New Connection Wizard
Your broadband connection should already be configured and ready to use. If your connection is not working properly, click the following link.
Learn more about broadband connections.
To close this wizard, click Finish.
< Back
Finish
Cancel

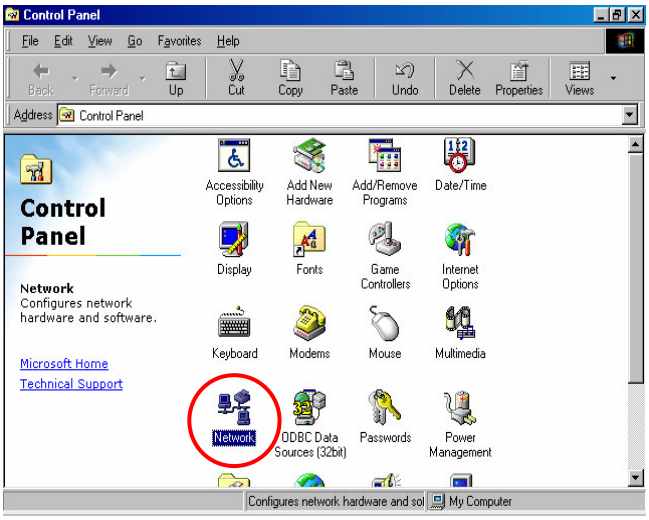
© 2008 4IPNET, INC.

- **TCP/IP Network Setup**

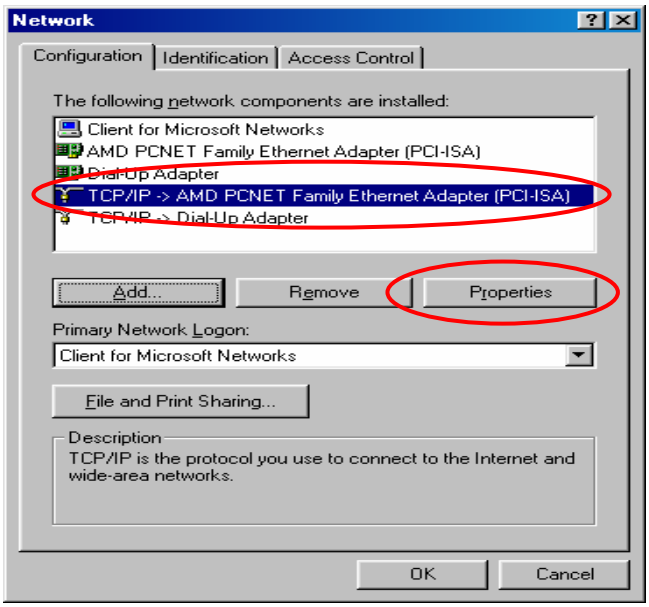
  If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any changes to directly start/restart the system. With the factory default settings, during the process of starting the system, 4ipnet WHG303 with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called **"Obtain an IP address automatically"**. If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

  - **Check the TCP/IP Setup of Window 9x/ME**

    1) Choose **Start** >> **Control Panel** >> **Network**.

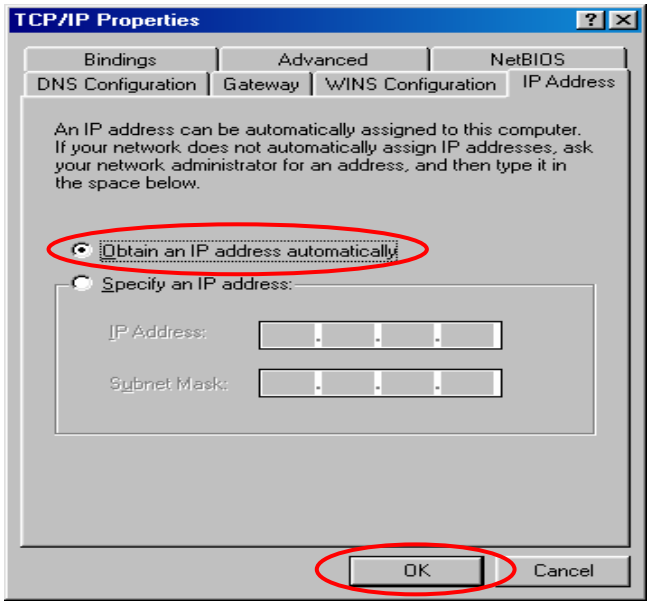


    2) Click on the **Configuration** tab and select **"TCP/IP** >> **AMD PCNET Family Ethernet Adapter (PCI-ISA)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



© 2008 4IPNET, INC.

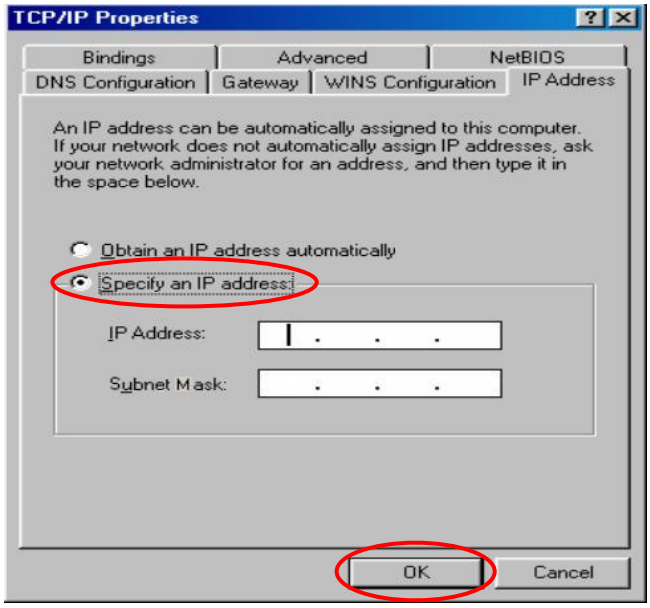
3) **Using DHCP:** If you want to use DHCP, click on the **IP Address** tab and choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WHG303.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

4) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WHG303.

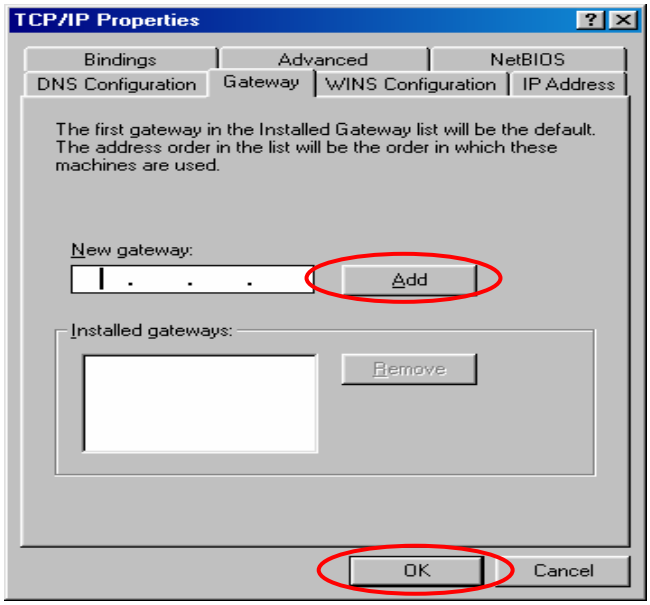
If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

4.1) Click on the **IP Address** tab and choose **"Specify an IP address"**. Enter the *IP Address*, *Subnet Mask* and then click ***OK***.

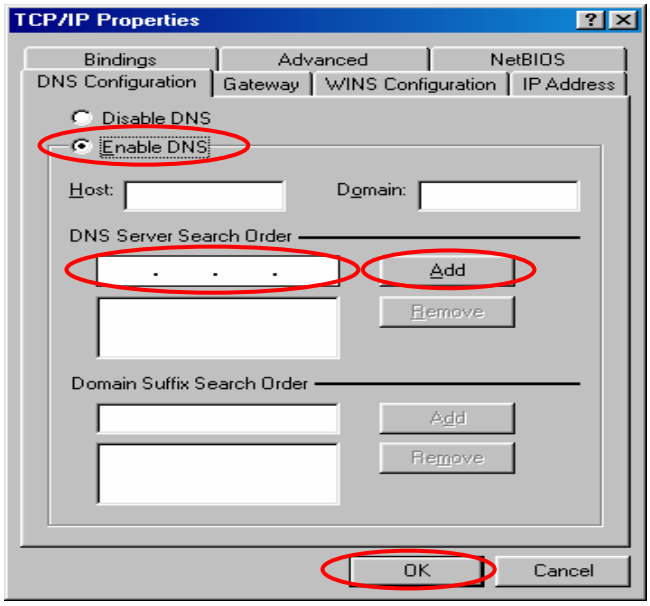

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

© 2008 4IPNET, INC.

4.2) Click on the **Gateway** tab. Enter the gateway address of WHG303 in the **"New gateway"** field and click ***Add***. Then, click ***OK***.

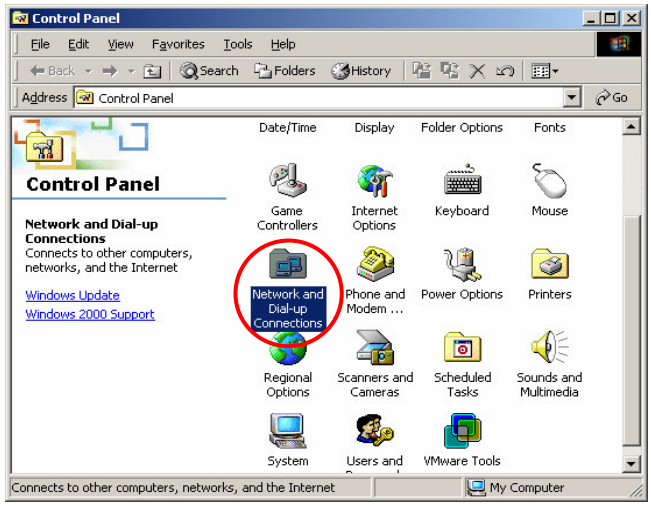


4.3) Click on **DNS Configuration** tab. If the DNS Server field is empty, select **"Enable DNS"** and enter *DNS Server address*. Click ***Add***, and then click ***OK*** to complete the configuration.



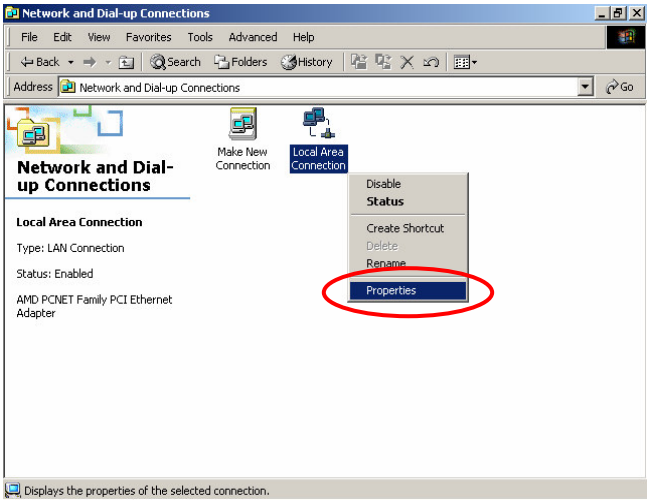
- **Check the TCP/IP Setup of Window 2000**

1) Select **Start** >> **Control Panel** >> **Network and Dial-up Connections**.

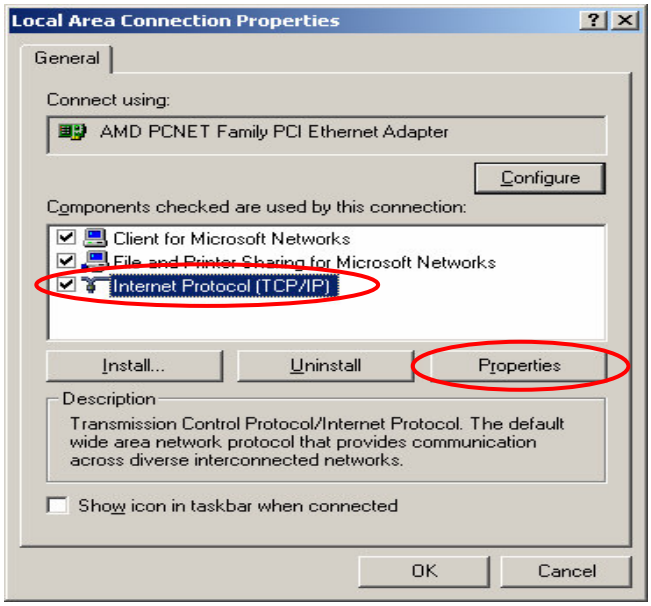


© 2008 4IPNET, INC.

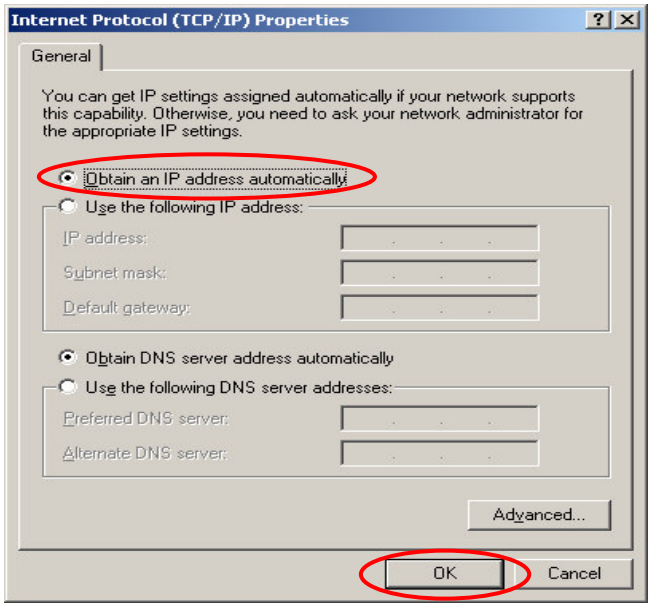
2) Right click on the **Local Area Connection** icon and select **"Properties"**.



3) Select **"Internet Protocol (TCP/IP)"** and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WHG303.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

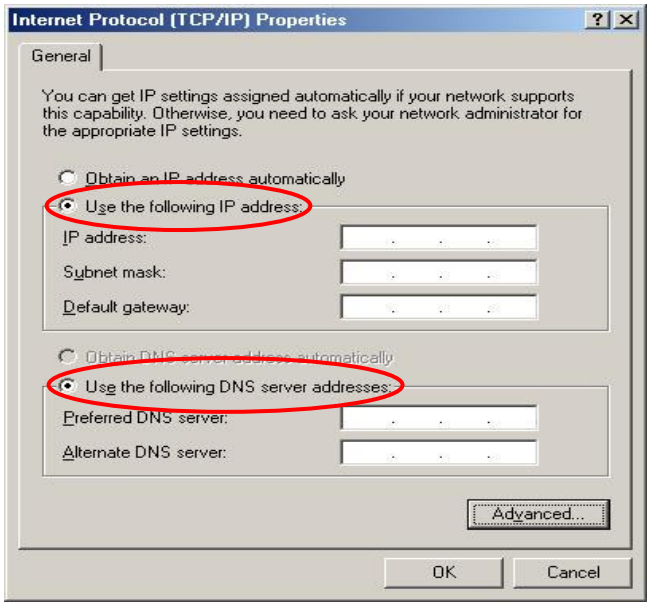
© 2008 4IPNET, INC.

5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WHG303.

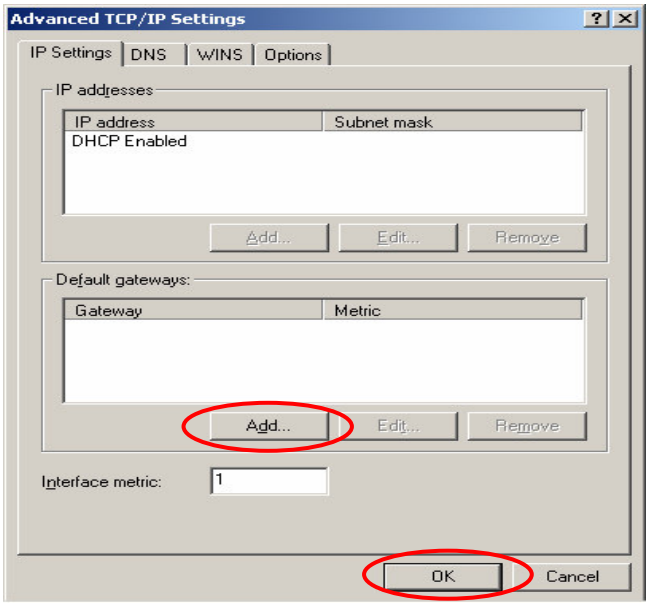
If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

5.2) Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.

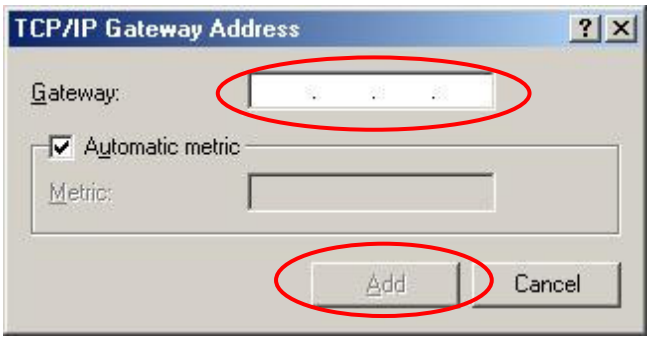

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

5.3) Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.



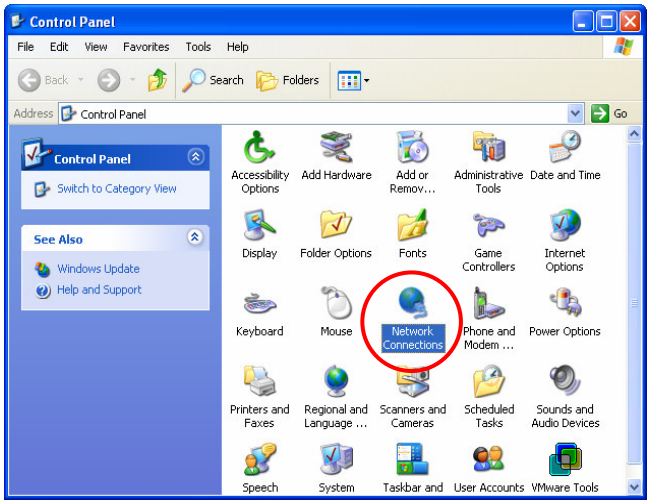
© 2008 4IPNET, INC.

5.4) Enter the gateway address of WHG303 in the **"Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to complete the configuration.

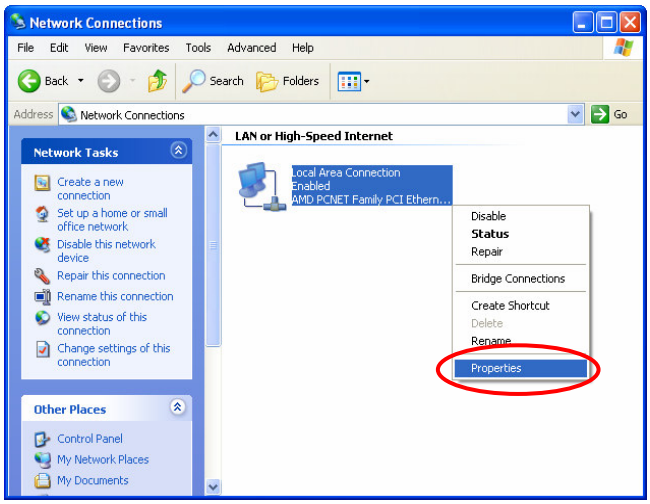


- **Check the TCP/IP Setup of Window XP**

1) Select **Start** >> **Control Panel** >> **Network Connection**.

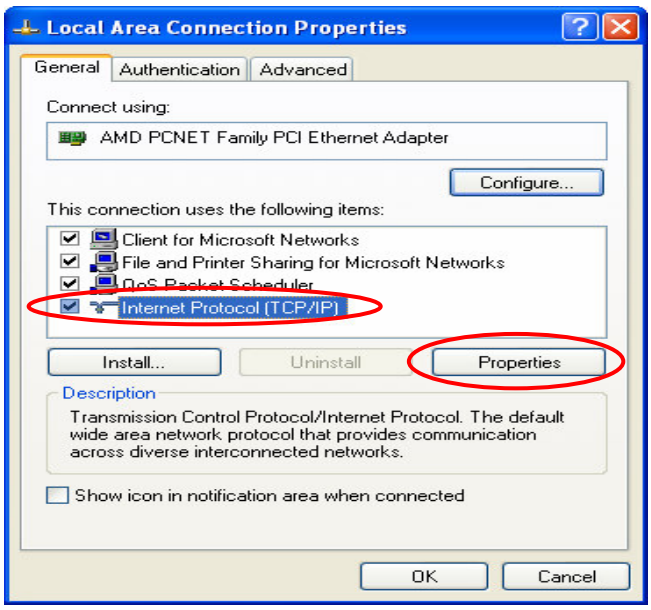


2) Right click on the **Local Area Connection** icon and select **"Properties"**.



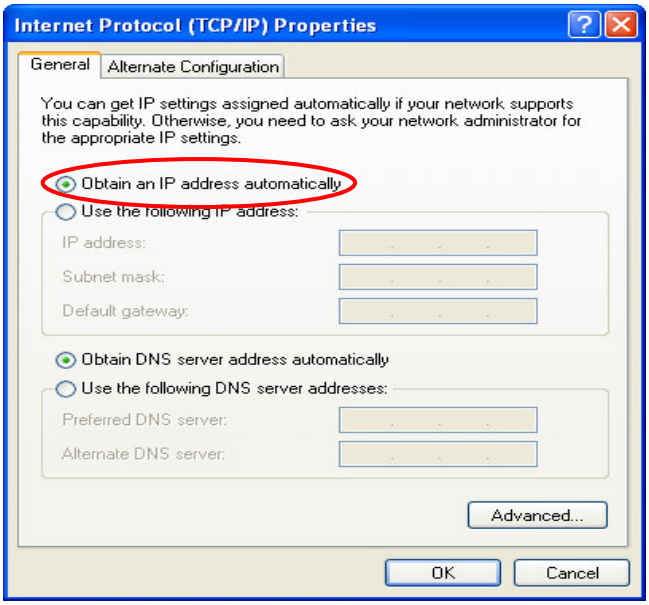
© 2008 4IPNET, INC.

3) Click on the **General** tab and choose **"Internet Protocol (TCP/IP)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WHG303.

5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WHG303.

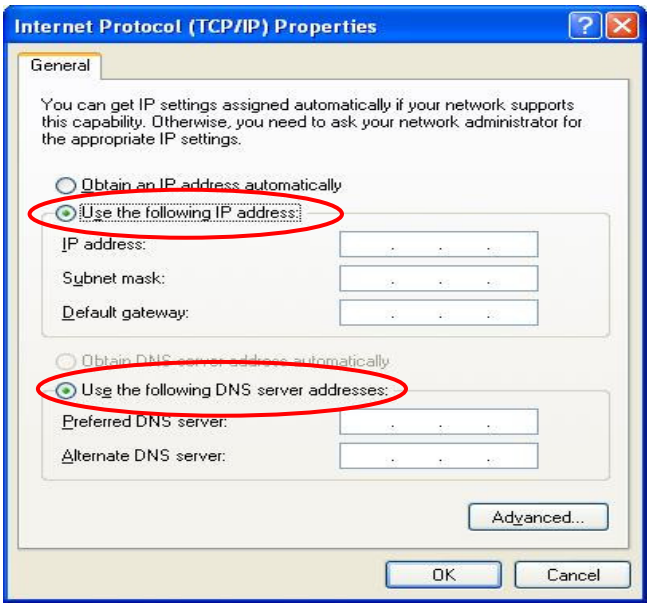

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

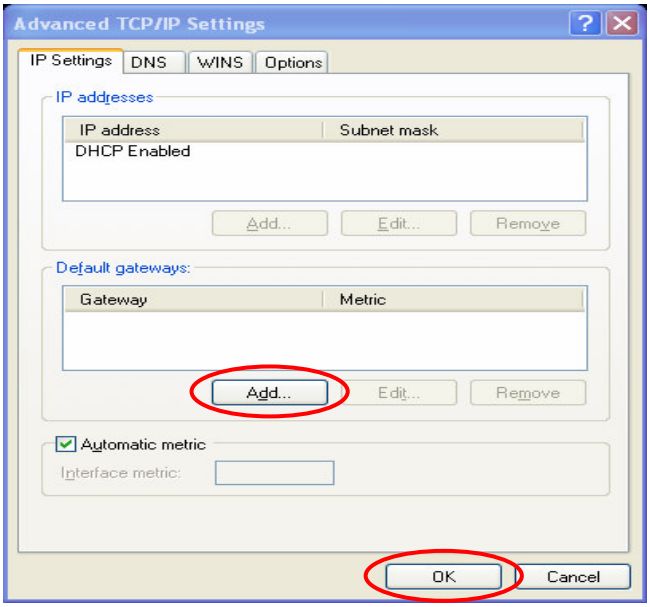
© 2008 4IPNET, INC.

5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

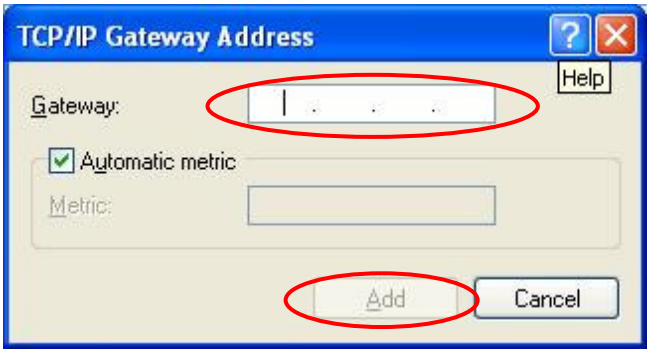
5.2) Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

5.3) Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.



5.4) Enter the gateway address of WHG303 in the *"***Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to finish the configuration.

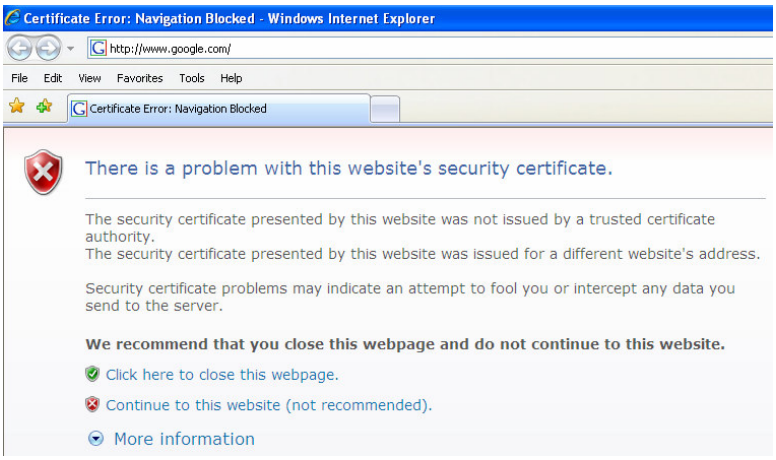


© 2008 4IPNET, INC.

▪ An Example of User Login

Normally, users will be authenticated before they get network access through WHG303. This section presents the basic authentication flow for end users. Please make sure that the WHG303 is configured properly and network related settings are done.

1. Open an Internet browser and try to connect to any website (in this example, we try to connect to www.google.com).
   a) For the first time, if the WHG303 is not using a trusted SSL certificate (for more information, please see *4.2.5 Additional Configuration*), there will be a "Certificate Error", because the browser treats WHG303 as an illegal website.


Certificate Error: Navigation Blocked - Windows Internet Explorer
http://www.google.com/
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

   b) Please press "Continue to this website" to continue.
   c) The default user login page will appear in the browser.

2. Enter the username and password (for example, we use a local user account: **test@local** here) and then click ***Submit*** button. If the ***Remember Me*** check box is checked, the browser will remember this user's name and password so that he/she can just click Submit next time he/she wants to login.
   Check the ***Remember Me*** box to store the username and password on the current computer in order to automatically login to the system at next login. Then, click the ***Submit*** button.
   The ***Remaining*** button on the **User Login Page** is for on-demand users only, where they can check their Remaining Usage time.

© 2008 4IPNET, INC.

3. Successful! The **Login Successful** page appearing means WHG303 has been installed and configured successfully. Now, you are connected to the network and Internet!

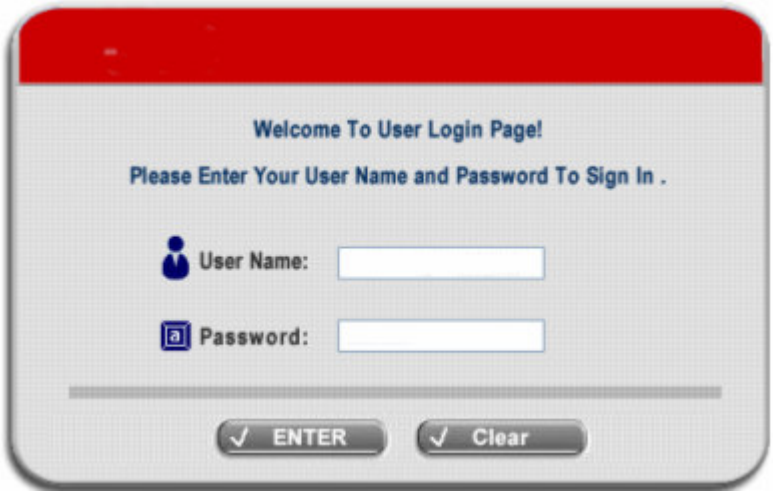
Note: When On-demand accounts are used (for example, we use **7ksc@ondemand** here), the system will display more information, as shown below.

© 2008 4IPNET, INC.

4. **Remaining Usage*:*** The remaining quota of this On-demand account that the user can surf the Internet.

Hello, you are logged in via 7ksc@ondemand
Please close this window or click this button to
Logout
Thank you!!
Remaining Usage:
5 Hour 59 Min 44 Sec
Login time: 2006-4-3 14:3:58
Redeem

5. **Redeem:** When the remaining quota is insufficient, the user can add up the quota by purchasing an additional account. Please enter the new username and password in the Redeem Page and click ***ENTER*** button to merge the two accounts so that there will be more quota for the original account.



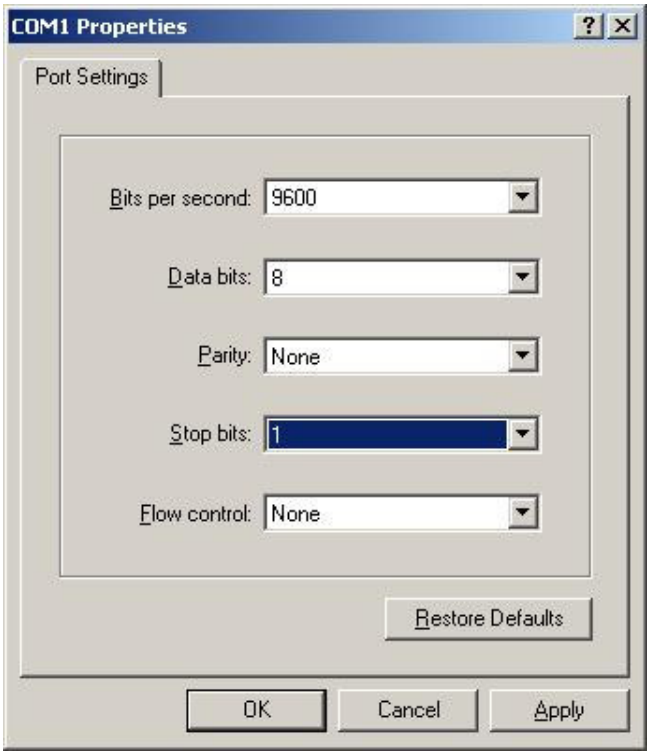
Note: The maximum session time/data transfer is 24305 days/9,999,999 Mbytes. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

© 2008 4IPNET, INC.

Appendix H. Console Interface

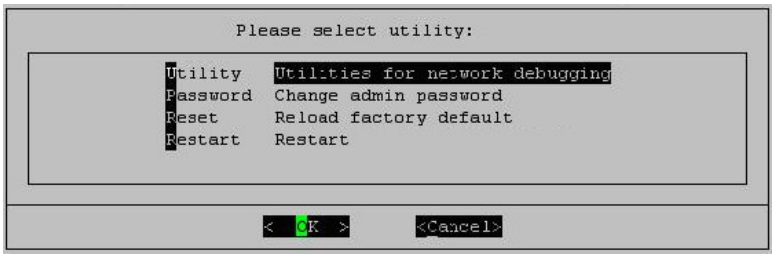
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. In order to connect to the console port of 4ipnet WHG303, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600,8,none,1, and none**.



*The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.*

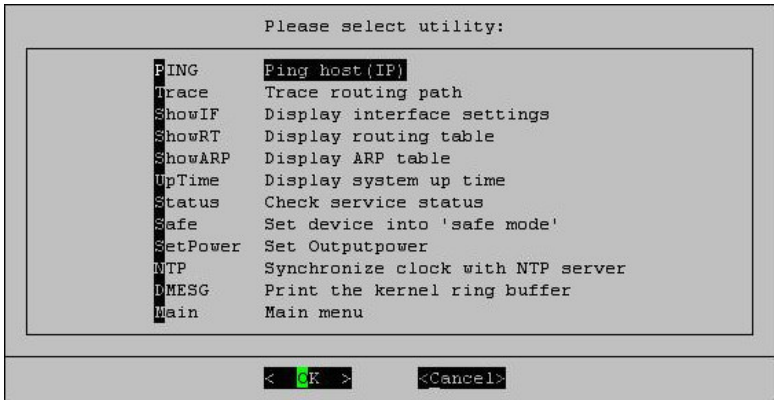
3. Once the console port of 4ipnet WHG303 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system, where the welcome screen or main menu should appear. If the welcome screen or main menu of the console still does not pop up, please check the connection of the cables and the settings of the terminal simulation program.



© 2008 4IPNET, INC.

- **Utilities for network debugging**

  The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follows:


Please select utility:
PING Ping host(IP)
Trace Trace routing path
ShowIF Display interface settings
ShowRT Display routing table
ShowARP Display ARP table
UpTime Display system up time
Status Check service status
Safe Set device into 'safe mode'
SetPower Set Outputpower
NTP Synchronize clock with NTP server
DMESG Print the kernel ring buffer
Main Main menu
< OK >
<Cancel>

  - Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
  - Trace routing path: Trace and inquire the routing path to a specific target.
  - Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
  - Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
  - Display ARP table: The internal ARP table of the system is displayed.
  - Display system up time: The system live time (time for system being turn on) is displayed.
  - Check service status: Check and display the status of the system.
  - Set device into "safe mode": If the administrator is unable to use Web Management Interface via browser for the system failed inexplicitly. The administrator can choose this utility and set it into safe mode, which enables him to manage this device with browser again.
  - Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
  - Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.
  - Main menu: Go back to the main menu.

© 2008 4IPNET, INC.

- **Change admin password**

  Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

  The username is "admin" and the default password is also "admin", which is the same as for the web management interface. Password can also be changed here. If administrators forget the password and are unable to log in the management interface from the web or the remote end of the SSH, they can still use the null modem to connect the console management interface and set the administrator's password again.

Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the 4ipnet WHG303 Admin username and password after logging in the system for the first time.

- **Reload factory default**

  Choosing this option will reset the system configuration to the factory defaults.

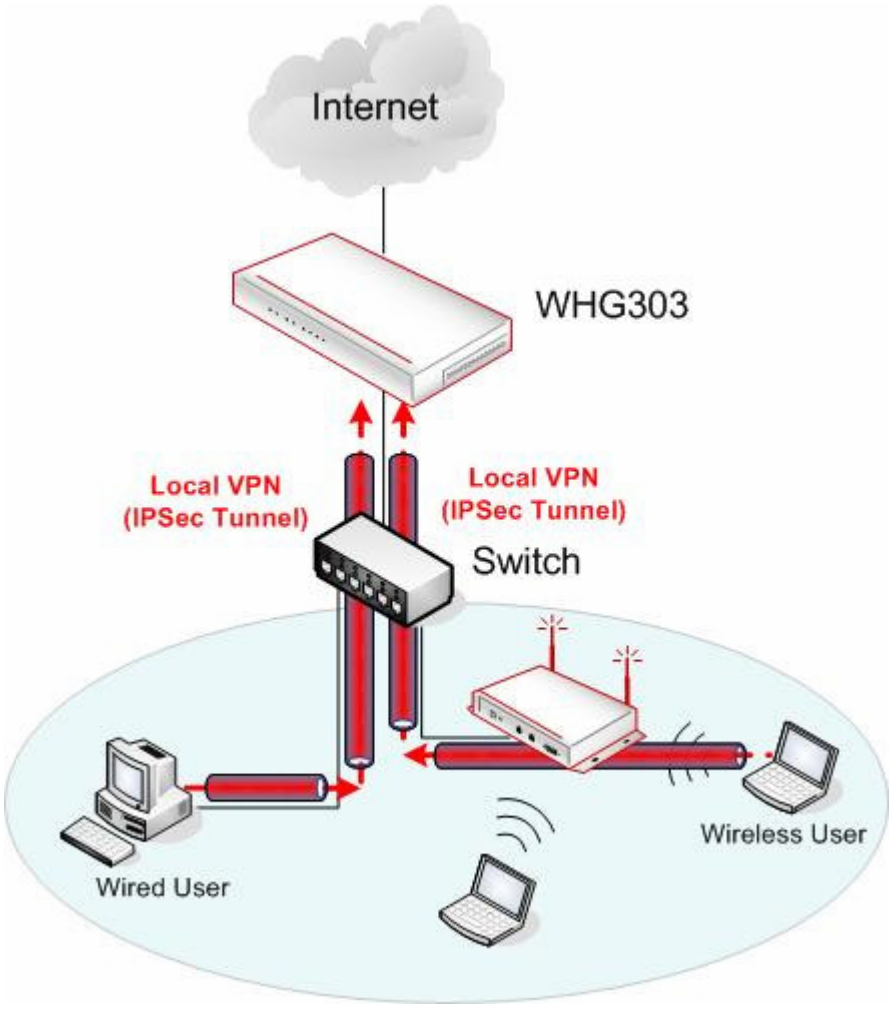
- **Restart 4ipnet WHG303**

  Choosing this option will restart 4ipnet WHG303.

© 2008 4IPNET, INC.

Appendix I. Local VPN

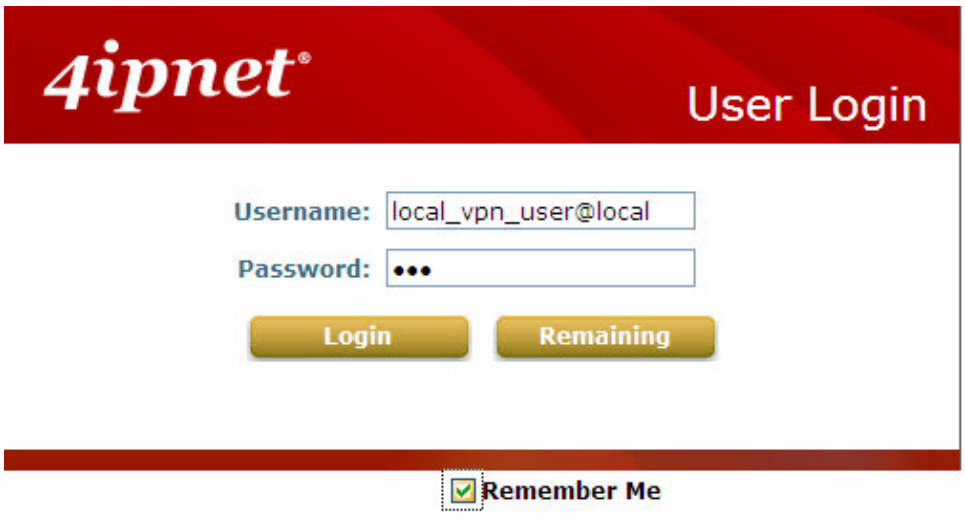
WHG303 has the ability to establish IPSec VPN tunnels between local user's Windows devices (on local wired or wireless network) and WHG303 itself, for the purpose of traffic protection on local networks. By pushing down ActiveX Control to the user's browser from WHG303, the system will be able to install a so-called "clientless" IPSec VPN.



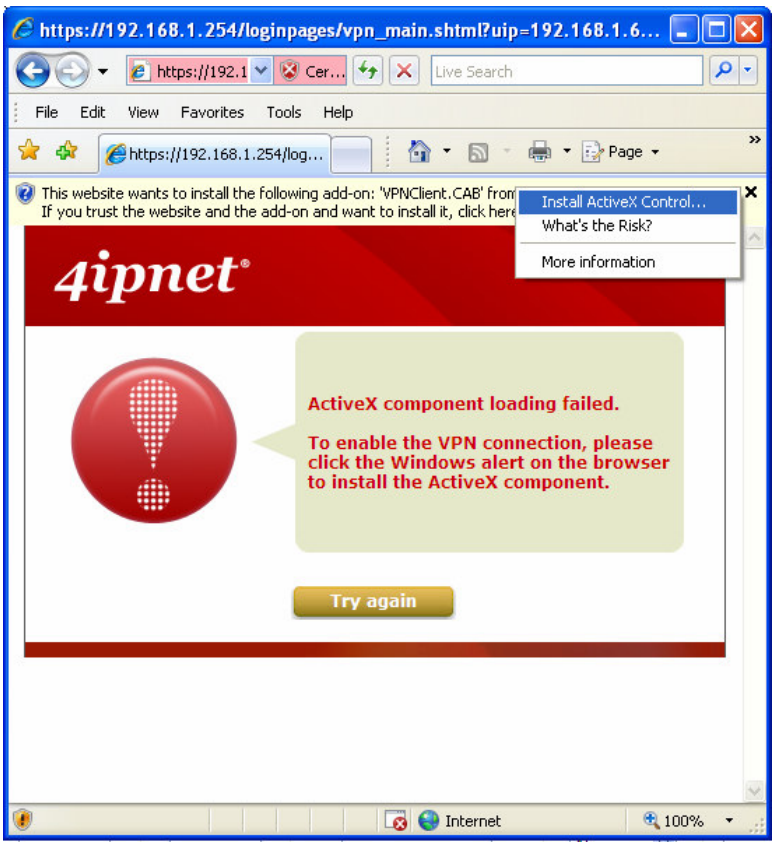
© 2008 4IPNET, INC.

1. User Operation Flow

a. As usual, enter username and password in the User Login Page



b. For the first time, if the user has never used Local VPN feature, Windows IE browser (6.0 or above) will display an alert message to ask the user whether she or he wants to install the "add-on" software.

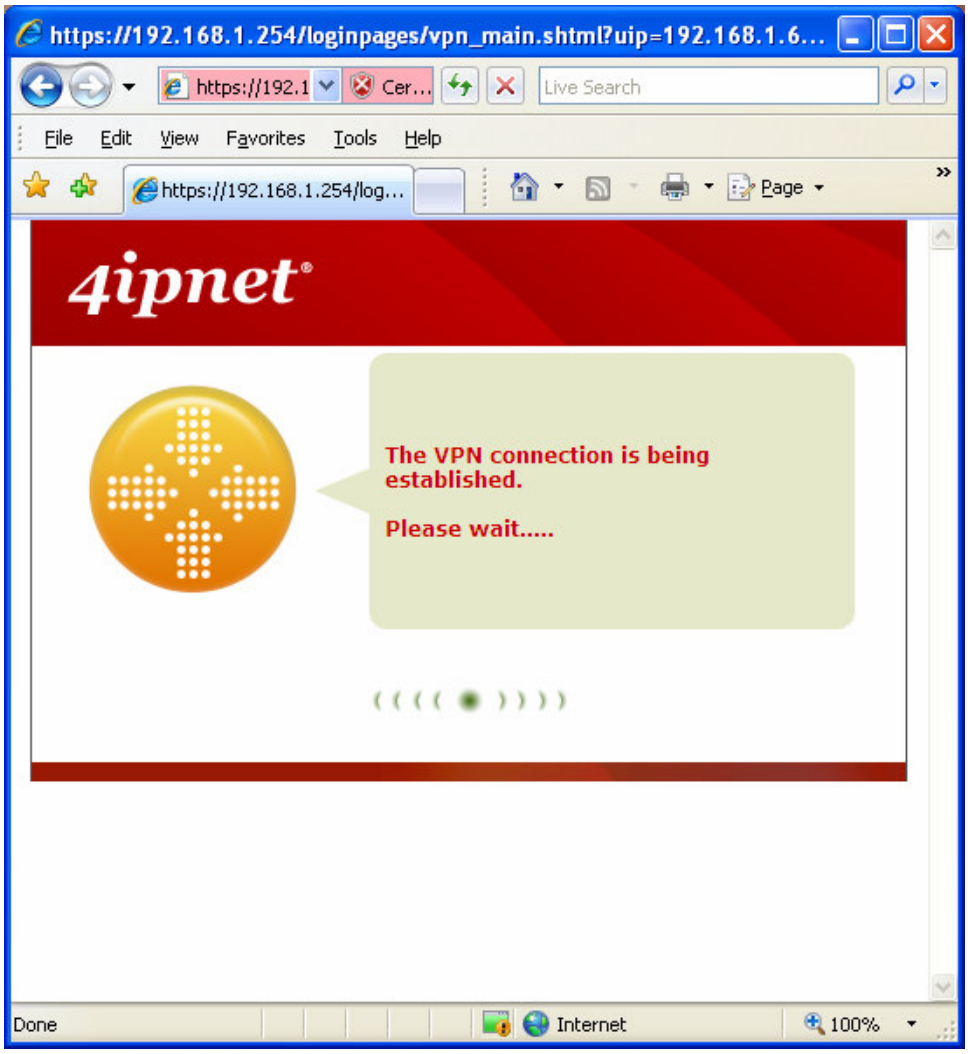


© 2008 4IPNET, INC.

c. Click on the alert message and then choose the "Install ActiveX Control" to install the software.

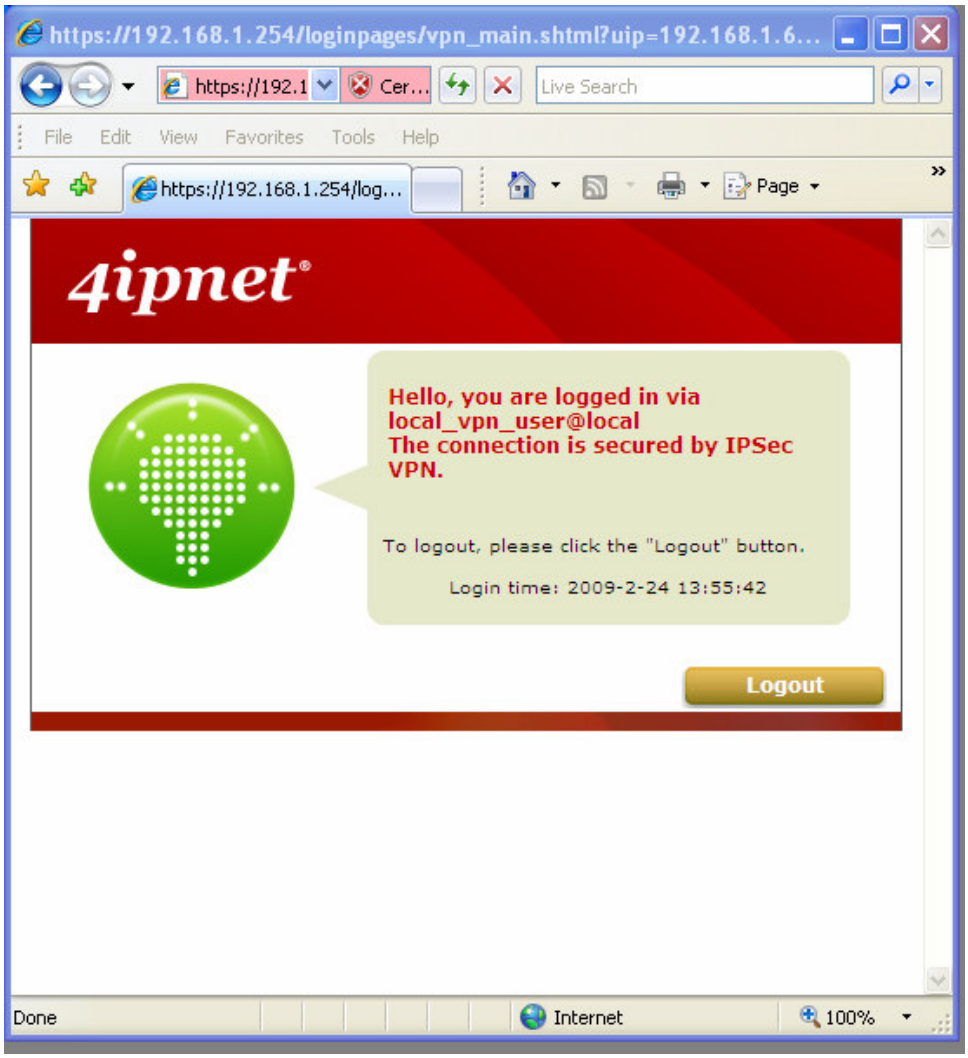
Internet Explorer - Security Warning
Do you want to install this software?
Name: VPNClient.CAB
Publisher: Cipherium Systems Co., Ltd.
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

d. After the software is installed well, the system will try to establish the IPSec VPN tunnel for the user automatically.



© 2008 4IPNET, INC.

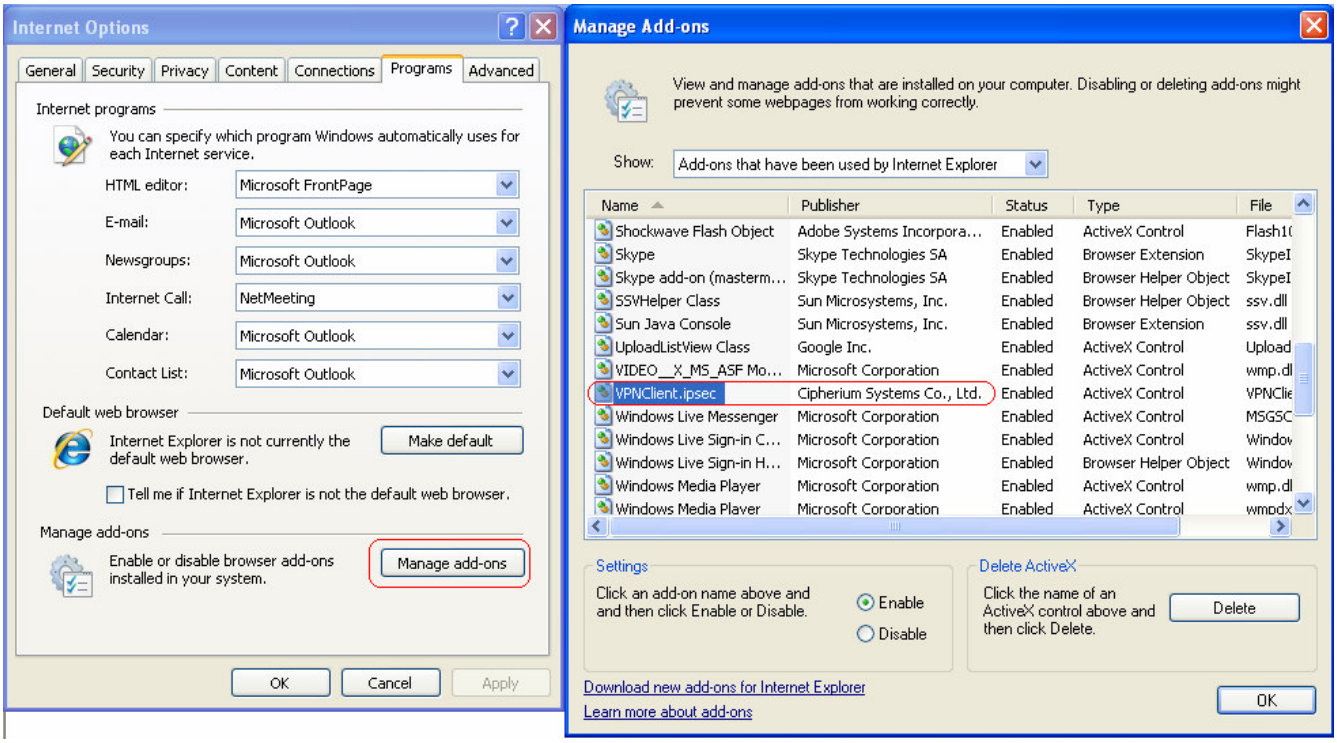
Once the IPSec VPN tunnel is established, the user has successfully logged in and the connection is secured by IPSec VPN.



2. ActiveX Control component

The ActiveX Control is a software component running inside Internet Explorer. The ActiveX Control component can be checked by the following windows.

© 2008 4IPNET, INC.



From Windows Internet Explorer, click "Manage add-ons" button inside "Programs" page under "Tools" to show the add-ons programs list. You can see VPNClient.ipsec was enabled.

© 2008 4IPNET, INC.

3. Limitations

The limitation of the client side due to ActiveX and Windows OS includes:

a. Internet Connection Firewall of Windows XP or Windows XP SP1 is not compatible with IPSec protocol. It shall be turned off to allow IPSec packets to pass through.

b. Without Windows patch KB889527, ICMP (Ping) and PORT command of FTP cannot work in Windows XP SP2.

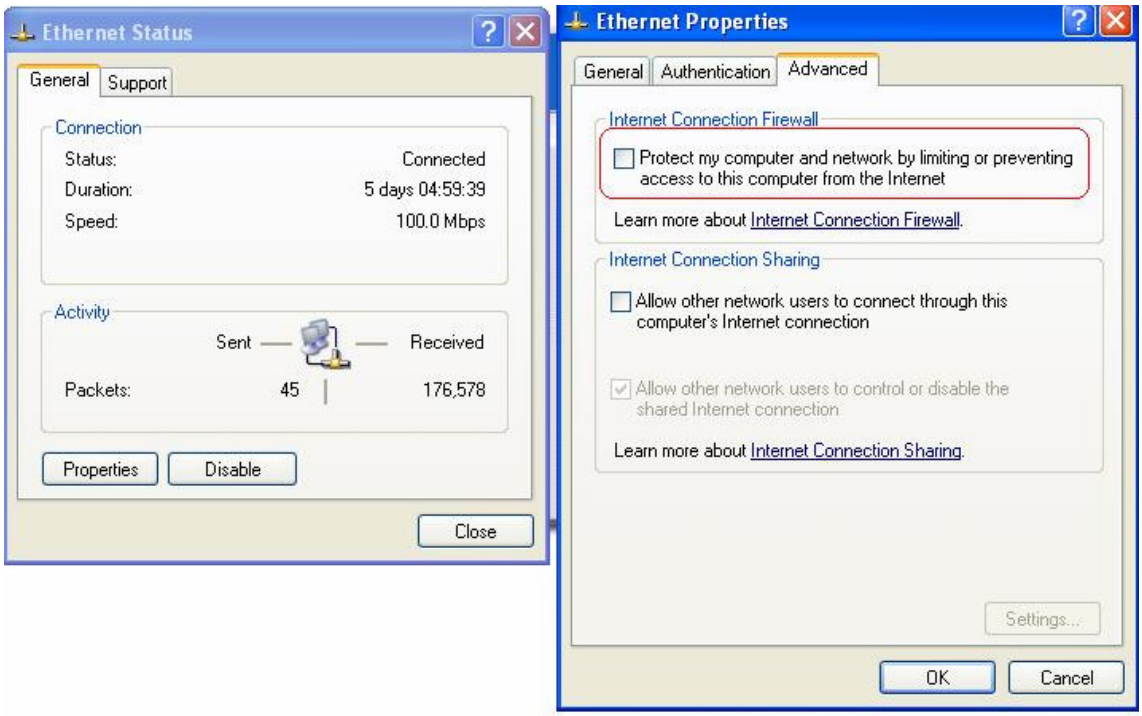
c. The forced termination (through CTRL+ALT+DEL or Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes IPSec tunnel can't be cleared properly at client's device. In this case, a reboot of client's device is needed to clear the IPSec tunnel.

d. The crash of Windows Internet Explorer may cause the same result.

e. There are some OS and browser which may not support Local VPN.

(1) Internet Connection Firewall

In Windows XP and Windows XP SP1, the Internet Connection Firewall is not compatible with IPSec. Internet Connection Firewall will drop packets from tunneling of IPSec VPN.



Suggestion: *Please* ***TURN OFF*** *Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.*

© 2008 4IPNET, INC.

(2) ICMP and Active Mode FTP

On Windows XP SP2 without patching by KB889527, it will drop ICMP packets from IPSec tunnel. This problem can be fixed by upgrading patch KB889527. Before enabling IPSec VPN function on client device, please access the patch from Microsoft's web at http://support.microsoft.com/default.aspx?scid=kb;en-us;889527.

This patch also fixes the problem of supporting active mode FTP inside IPSec VPN tunnel of Windows XP SP2.

Suggestion: *Please UPDATE client's Windows XP SP2 with this patch.*

(3) The Termination of ActiveX

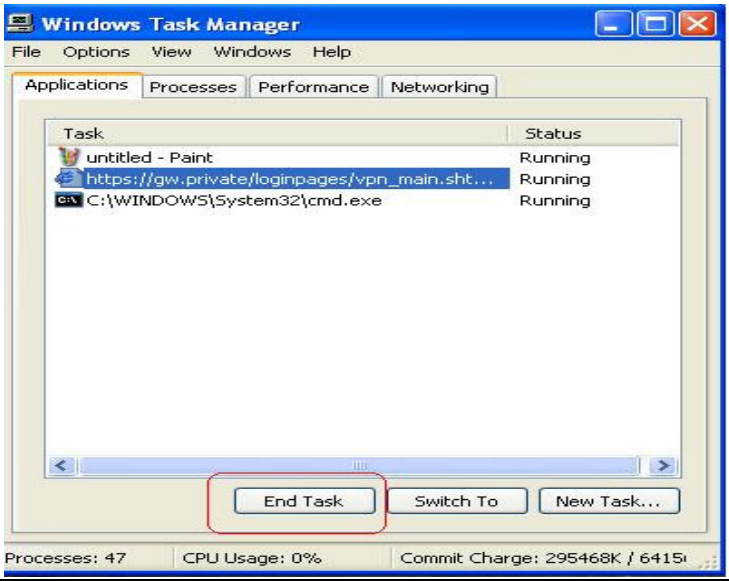
The ActiveX component for IPSec VPN is running paralleled with the web page of "Login Success". Unless user decides to close the session and to disconnect with WHG303, the following conditions or behaviors of using browser shall be avoided in order to maintain the built IPSec VPN tunnel always alive.

Reasons may cause the Internet Explorer to stop the ActiveX unexpectedly as follows:

The crash of Internet Explorer on running ActiveX

Suggestion: *Please reboot client's computer, once Windows service is resumed, go through the login process again.*

Terminate the Internet Explorer Task from Windows Task Manager


Windows Task Manager
File Options View Windows Help
Applications Processes Performance Networking
Task Status
untitled - Paint Running
https://gw.private/loginpages/vpn_main.sht... Running
C:\WINDOWS\System32\cmd.exe Running
End Task Switch To New Task...
Processes: 47 CPU Usage: 0% Commit Charge: 295468K / 6415

Suggestion: *Don't terminate this VPN task of Internet Explorer.*

© 2008 4IPNET, INC.

There are some cases of Windows messages by which WHG303 will warn current user to:

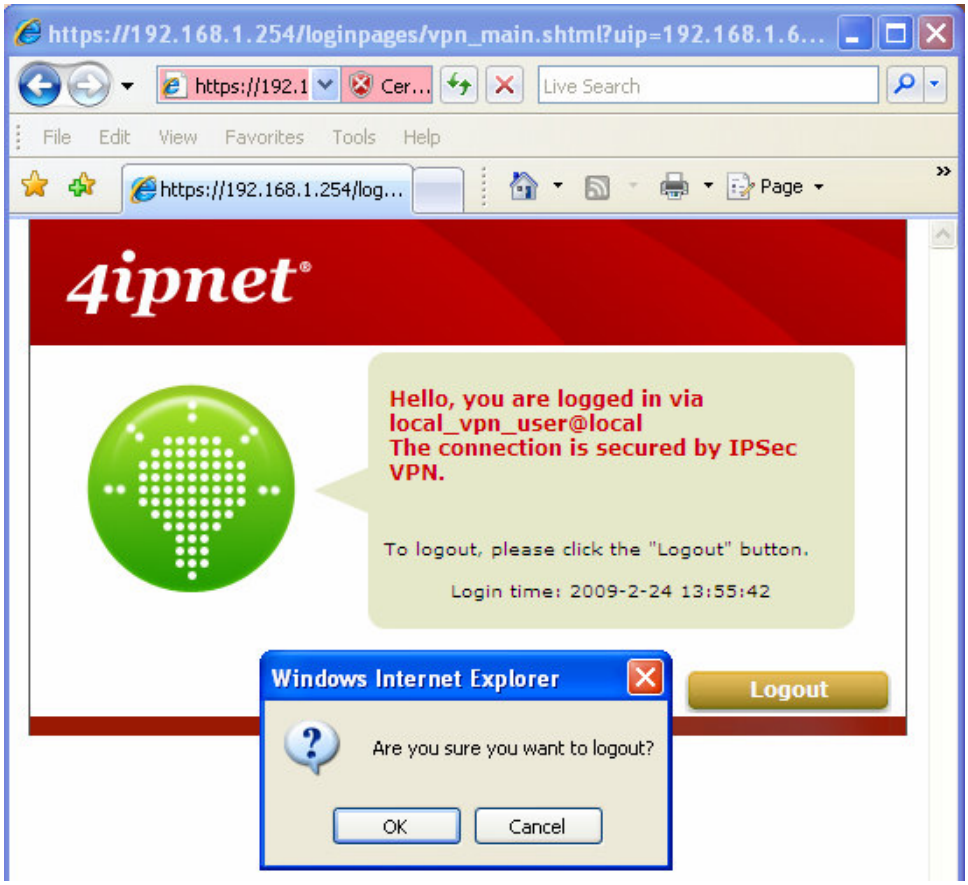
① Close the Windows Internet Explorer,

② Click "logout" button on "login success" page,

③ Click "back" or "refresh" of the same Internet Explorer,

④ Enter new URL in the same Internet Explorer,

⑤ Open a URL from the other application (e.g. email of Outlook) that occupies this existing Internet Explorer.



That shall all cause the termination of IPSec VPN tunneling if user chooses to click "Yes". The user has to log in again to regain the network access.

Suggestion: *Click "Cancel" if you do not intend to stop the IPSec VPN connection yet.*

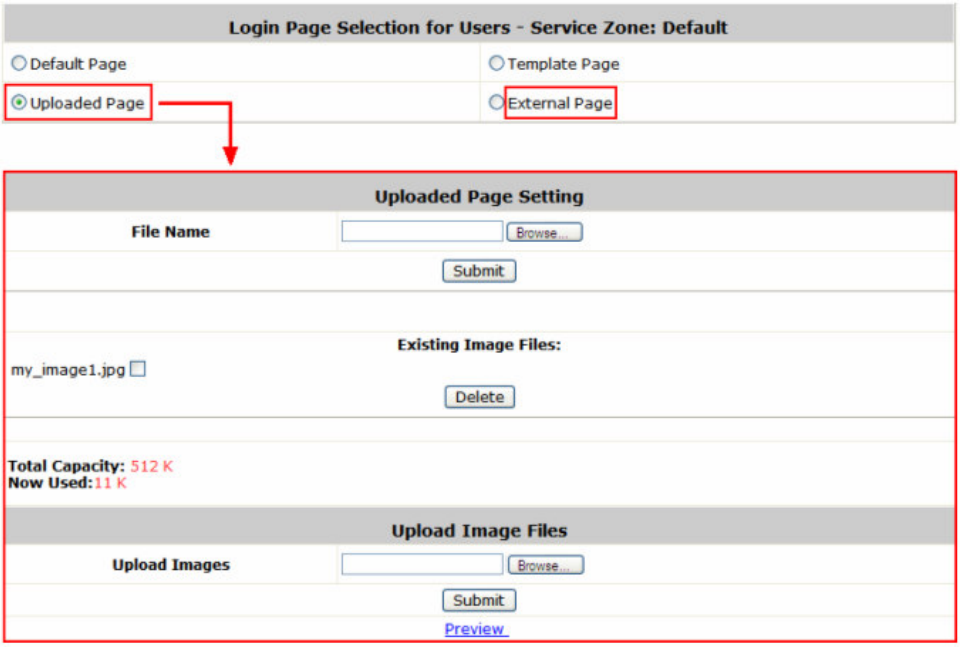
© 2008 4IPNET, INC.

Appendix J. Customizable Pages

The system allows administrators to customize web pages (*Login Page*, *Logout Page*, *Login Success Page*, *Login Success Page for On-demand User*, and *Logout Success Page*) that will be displayed in end users' browsers during login and logout process. As an example, this section will guide you through making a custom *Login Page* – editing the HTML code and uploading related files to the system.

1. Basics

(a) Each *Service Zone* can have its own *Login Page* using four different options, as shown below (for *Default Service Zone*, click *Main Menu* > > *System* >> *Service Zone* >> Configure *Default Service Zone* >> Configure *Login Page*).



A customized *Login Page* can be uploaded to the system (**Uploaded Page** option) or put in an external web server (**External Page** option). Note that **Default Page** and **Template Page** are options which do not require administrators to edit the HTML code.

(b) With the **Uploaded Page** option selected, administrators have to upload the *Login Page* itself (HTML code) as well as related image files which are used in the HTML code.

(c) It is recommended to use the HTML code of *Default Login Page* as a starting point to customize your own *Login Page*. To get the HTML code, right click on the hyperlink **Preview** and use "Save Target As" to save the code.

© 2008 4IPNET, INC.

2. Processing the HTML code

For the login process to work appropriately, some elements are required to be kept in the HTML code, while some elements are optional, depending on whether On-demand accounts are used.

(a) Required elements in the HTML code include:

- HTML form #1 that allows the user to enter information (username and password):

```
<form action="userlogin.shtml" method="post" name="login" id="login">
…
<input class="textinput" name="myusername" id="myusername" type="text" size="24"
onKeyPress="return submitenter(this, event);">
…
<input class="textinput" name="mypassword" id="mypassword" type="password" size="24"
onKeyPress="return submitenter(this, event);">
…
</form>
```

- Hyperlink (or HTML button element) in HTML form #1 that allows the user to submit information:

```
<form action="userlogin.shtml" method="post" name="login" id="login">
…
<a href="JavaScript:Form_Submit(login);" class="appmsg">Login</a>
…
</form>
```

- HTML form #2 that allows the browser to process information, as needed, about *On-demand* users:

```
<form action="reminder.shtml" method="post" name="Reminder">
<input type=hidden name=myusername value="">
<input type=hidden name=mypassword value="">
</form>
```

- All JavaScript functions that will be executed by the browser when needed:

```
<script language="JavaScript1.2">
…
function functionname(var1,var2,...,varX)
{
some code
}
…
</script>
```


© 2008 4IPNET, INC.

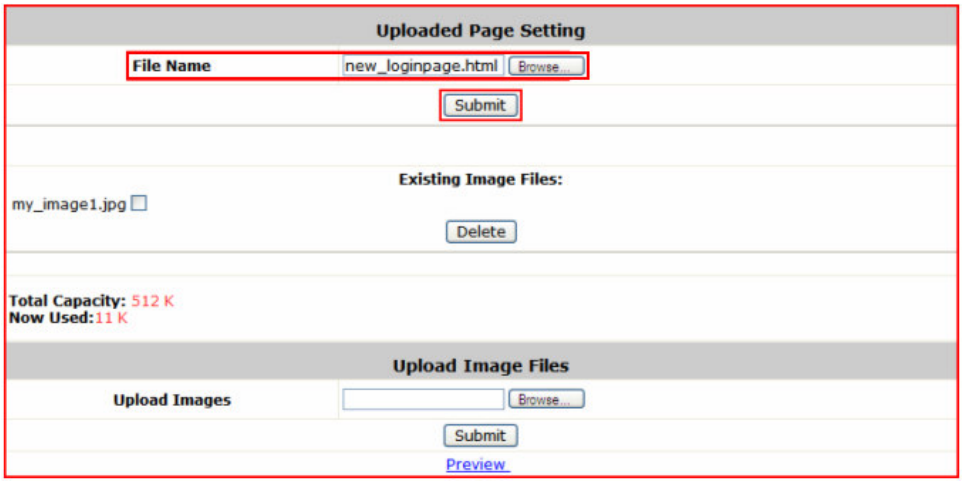
(b) Optional elements in the HTML code

- Input tag "rememberme" ("Remember Me" checkbox) in HTML form #1 that can be used to allow the browser to save username and password, when this function is selected

```
<form action="userlogin.shtml" method="post" name="login" id="login">
…
<input class="textinput" type="checkbox" id="rememberme" name="rememberme">
…
</form>
```

(c) Upload the HTML code

- Example: we have finished editing the HTML code and saved it as *new_loginpage.html*. Then it should be uploaded to the system manually, as shown below.



3. Processing the image files

(a) In the HTML code, "***../images/***" specifies the path of default **system** image folder, while "***imagesZ/***" specifies the path of **uploaded** image folder, where ***Z*** is the number of *Service Zone* (0 is *Default Service Zone*, 1 is *Service Zone #1*, 2 is *Service Zone #2*, etc.). The following are some examples.

- Example 1: to use *apply.gif* in the system image folder as a background image, we should specify *background="../images/apply.gif"*

```
<form action="userlogin.shtml" method="post" name="login" id="login">
…
<td width="125" height="28" align="center" background="../images/apply.gif" valign="middle">
…
</form>
```


© 2008 4IPNET, INC.

- Example 2: to use *my_image1.jpg* in the uploaded image folder of *Default Service Zone*, we should specify *<img src="images0/my_image1.jpg">*

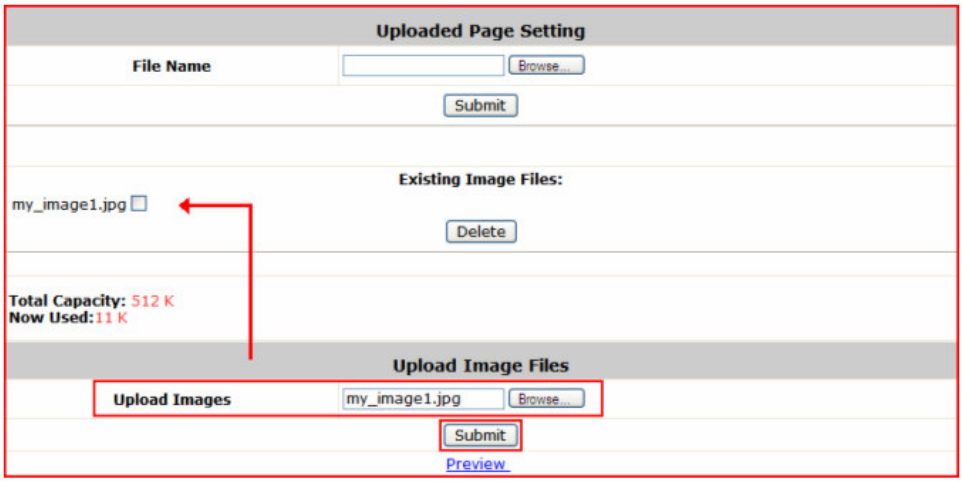
```
<form action="userlogin.shtml" method="post" name="login" id="login">
…
<img src="images0/my_image1.jpg">
…
</form>
```

- Example 3: to use *my_image1.jpg* in the uploaded image folder of *Default Service Zone* and *my_image3.jpg* in the uploaded folder of *Service Zone #1*, we should specify *<img src="images0/my_image1.jpg">* and *<img src="images1/my_image3.jpg">*

```
<form action="userlogin.shtml" method="post" name="login" id="login">
…
<img src="images0/my_image1.jpg">
…
<img src="images1/my_image3.jpg">
…
</form>
```

(b) Upload the image files

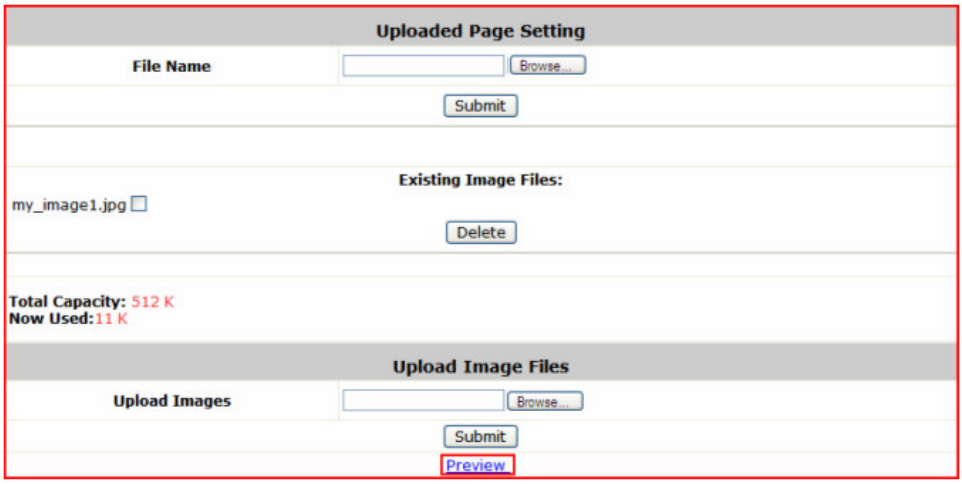
- Example: the HTML code uses *<img src="images0/my_image1.jpg">*. The file *my_image1.jpg* should be manually uploaded to the uploaded image folder of *Default Service Zone*, as shown below.



© 2008 4IPNET, INC.

4. Preview the new Login Page

After the HTML code and image files are uploaded successfully, to view how the new *Login Page* looks in the browser, click on the hyperlink **Preview**.



Note: *For a simple example of editing HTML code, please see another file "Custom_Login_Page_Sample_Code".*

Appendix K. RADIUS Accounting

The Vendor Specific Attributes (VSA) values are intended to provide service providers with information such as the user's location to facilitate back-end processing of transaction data as well as to provide service-level information.

The system now supports a VSA value for session control. This implemented VSA value is the amount of data a user is allowed to transfer (download + upload) per session. When the RADIUS server accepts the gateway's authentication request, the RADIUS server will reply with this attribute value inside the *Access-Accept* packet. Accordingly, the gateway will be able to control the user's session.

The following is the summary of this vendor-specific attribute: (the fields are transmitted from left to right)

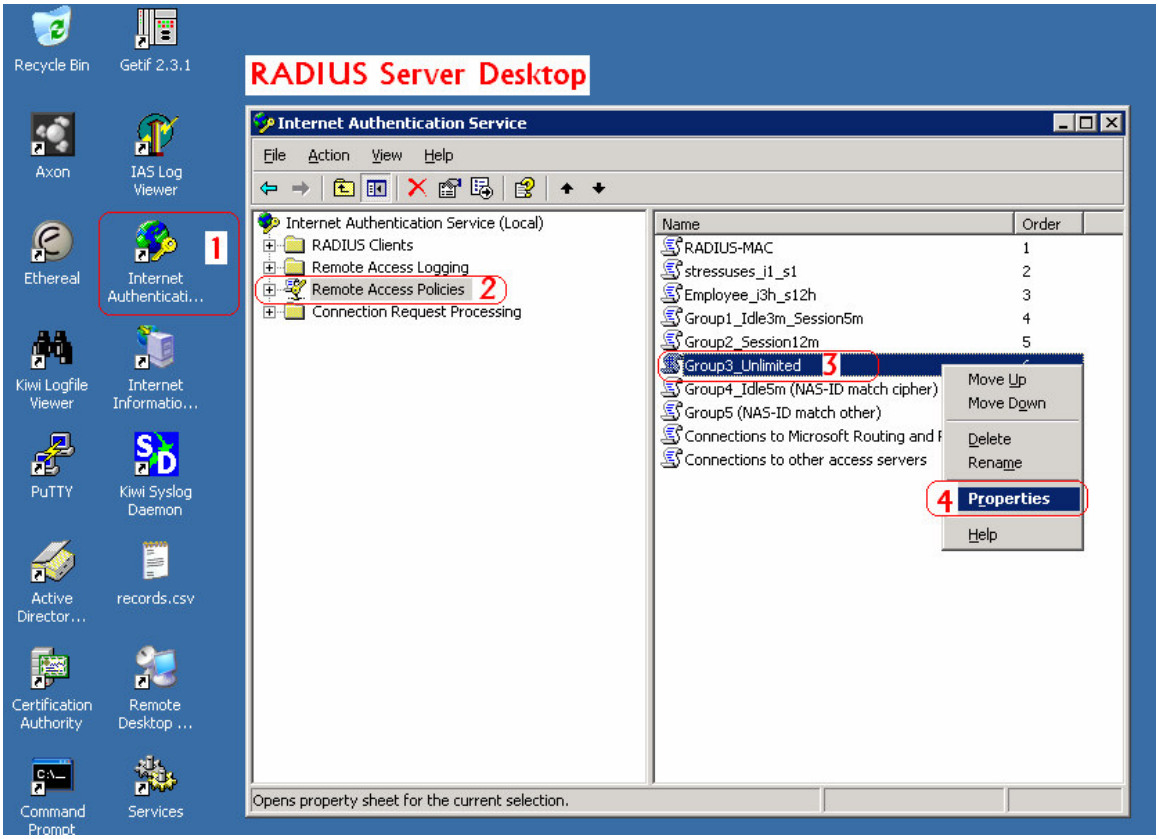
Vendor Specific Attribute Number (By RADIUS Standard)	Vendor Code (By vendor)	Vendor Assigned Attribute Number (By vendor)	Attribute Value (Maximum traffic count, bytes in hexadecimal, allowed to transfer per session)
26	**31932**	**10**	**By local administrator (Ex: 0x100000)**

- **Configuring VSA on RADIUS server**

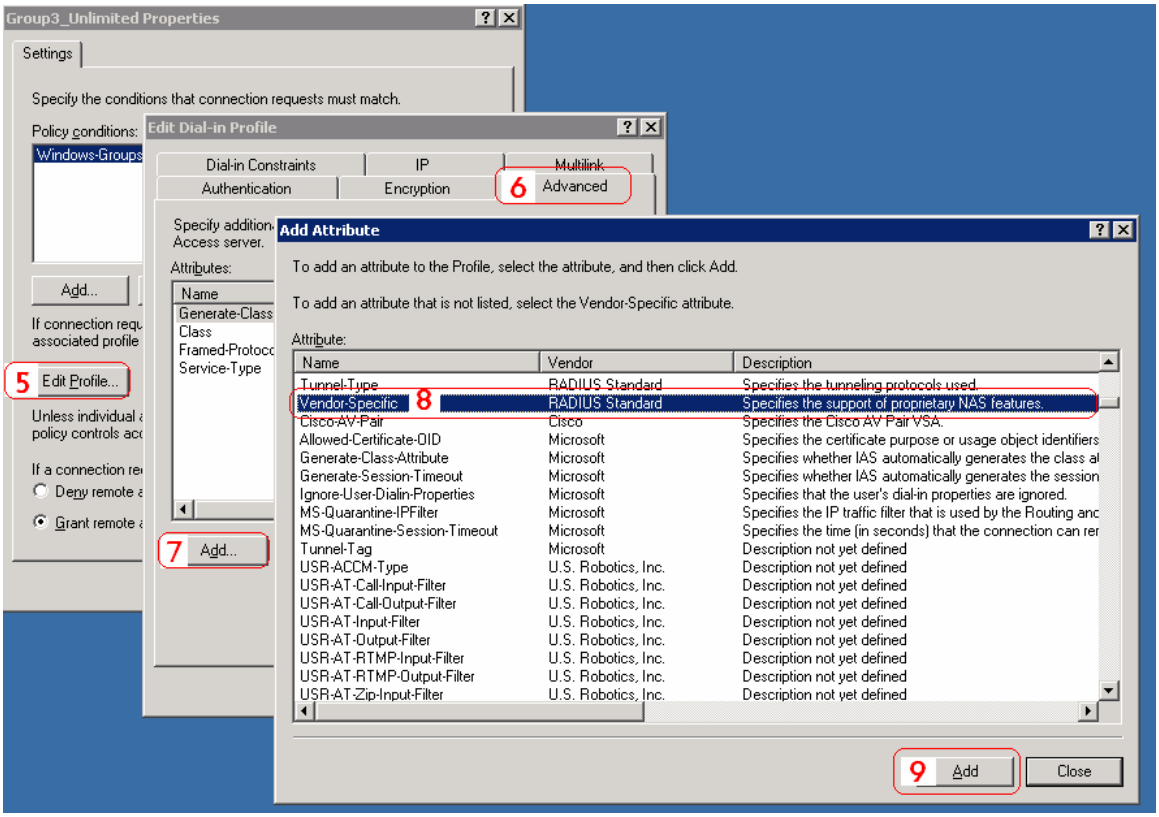
This section will guide you through a VSA configuration in the external RADIUS server. Before getting started, go to or remotely connect to the external RADIUS server's desktop.

© 2008 4IPNET, INC.

Step 1 to 4: Run "Internet Authentication Server", open "Remote Access Policies" and select a policy. Right click and scroll down to its properties page.

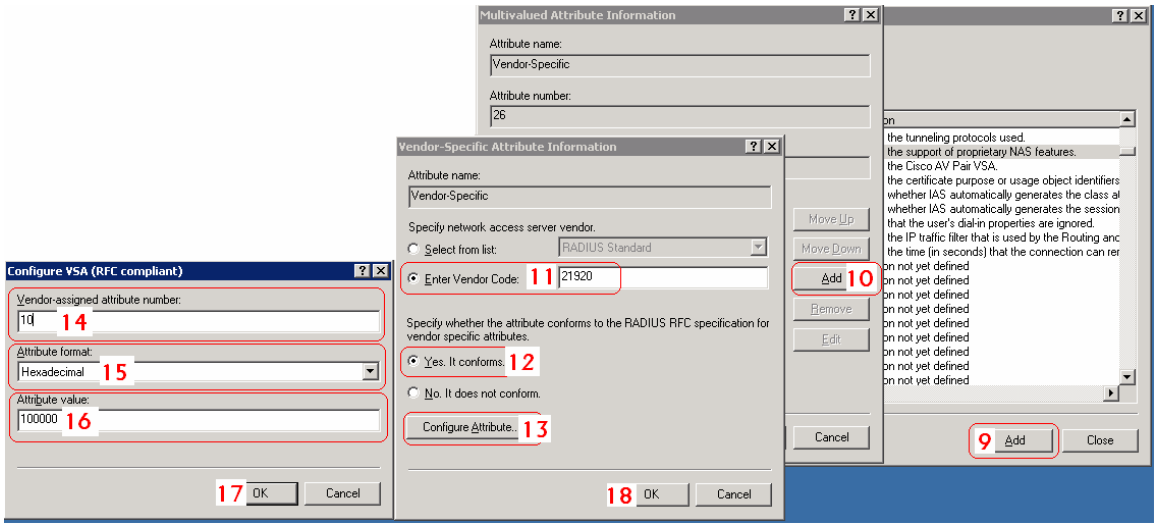


Step 5 to 9: Adding a "Vendor-Specific" attribute into properties of this selected policy.

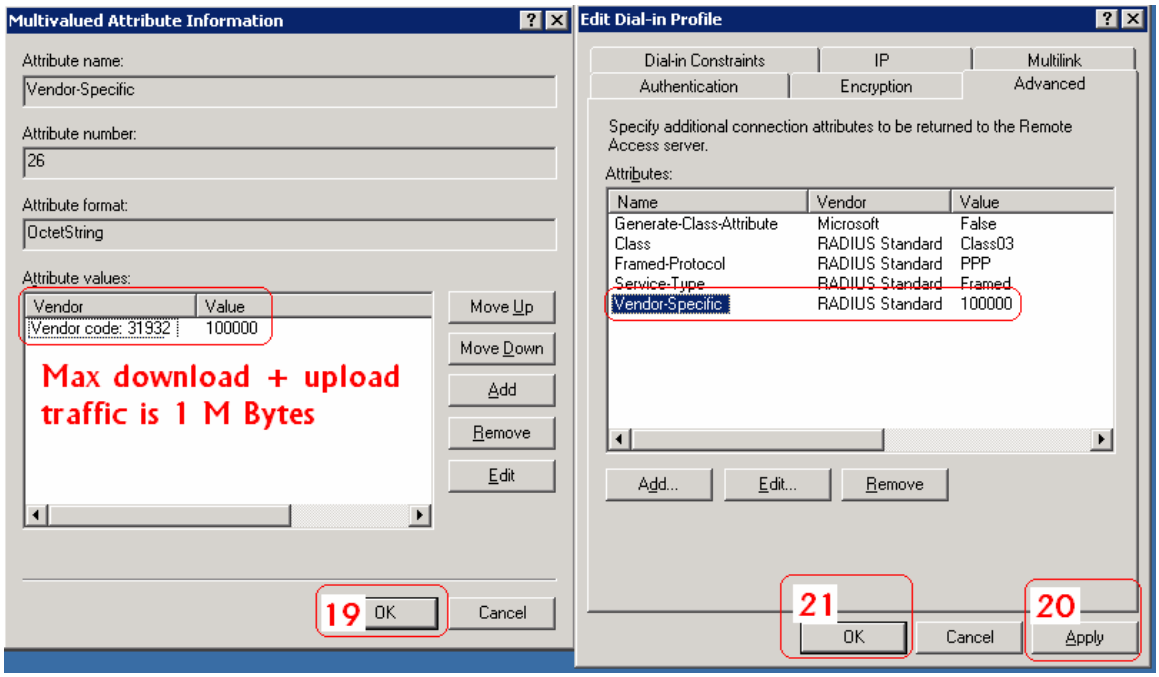


© 2008 4IPNET, INC.

Step 9 to 18: Adding "Vendor Code = 31932", "Vendor-assigned attribute number = 10", and "Attribute Value = 100000 in Hexadecimal" into properties of this policy.



Step 19 to 21: Shows that the Attribute Value has been added.



- **Creating a user in Active Directory**

This section will show you how to create a user and add it into a group in Active Directory.

Step 1. Open "Active Directory"

Step 2. Go to container "Users"

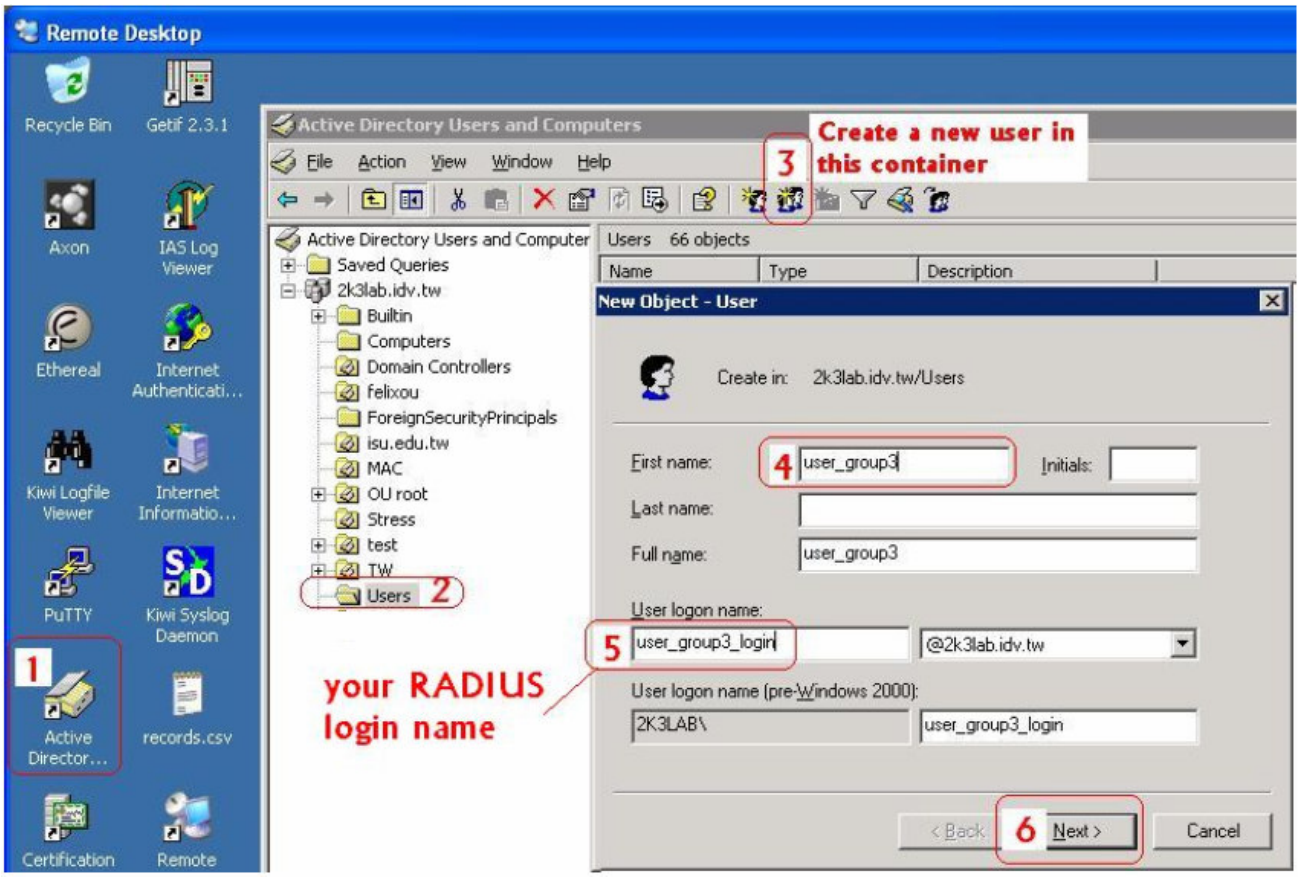
Step 3. Create a new user in this container.

Step 4. Enter the first name of this user.

Step 5. Enter User logon name which is the login name you will use in your RADIUS server.

© 2008 4IPNET, INC.

Step 6. Click "Next" to continue.

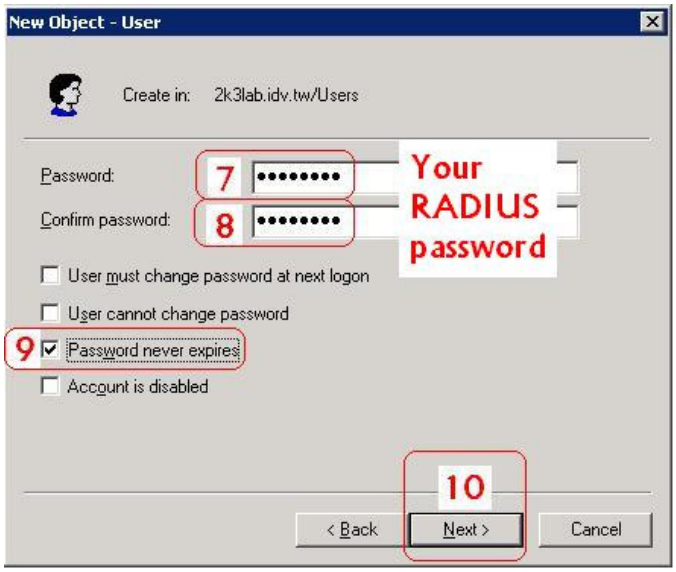


Step 7. Enter your RADIUS password

Step 8. Re-enter your RADIUS password

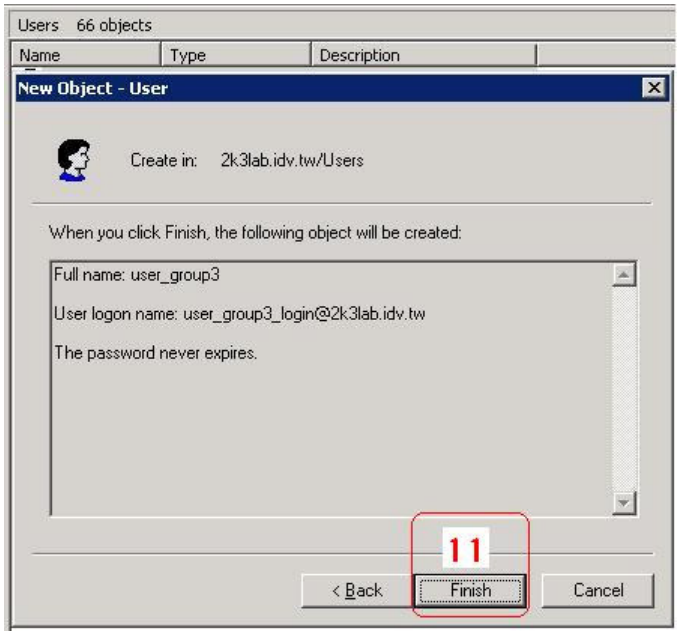
Step 9. Check "Password never expires" so that this password lasts.

Step 10. Click Next to continue.



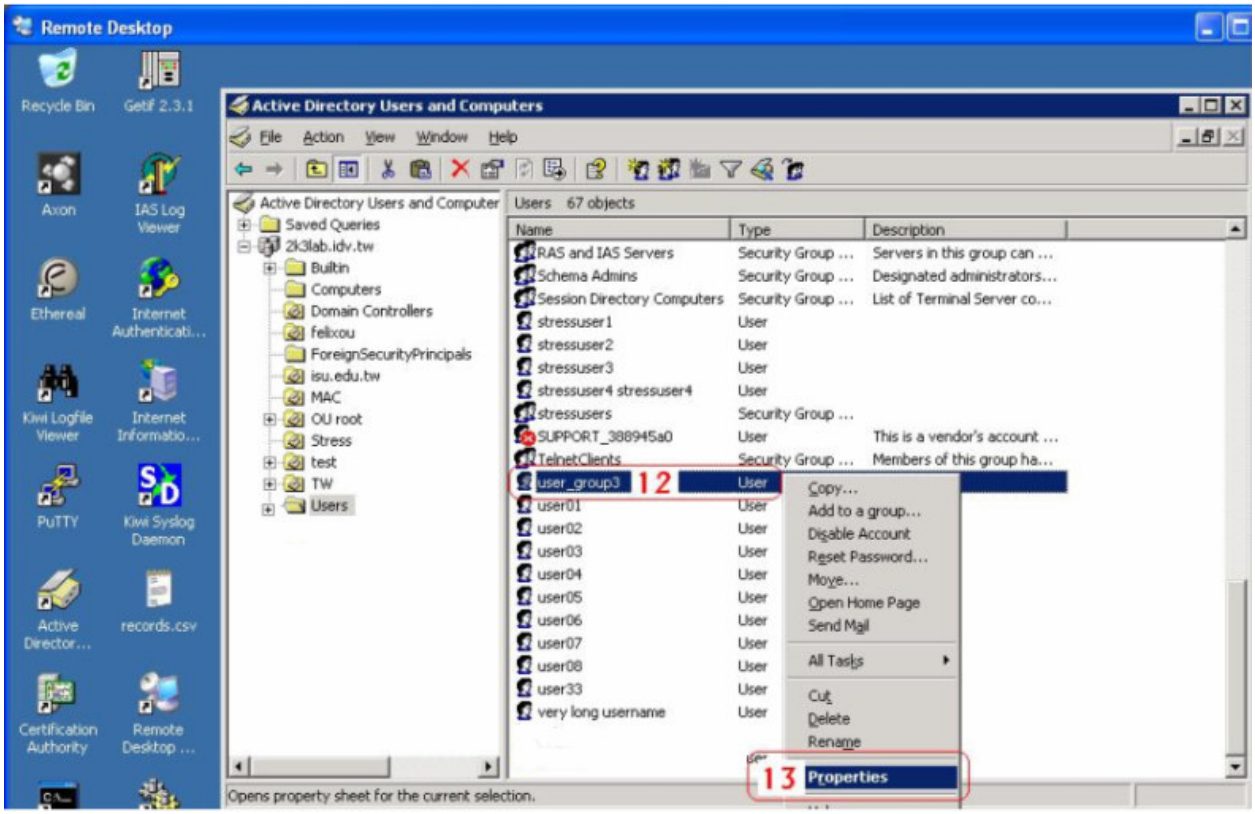
Step 11. Click finish to get done with account creation.

© 2008 4IPNET, INC.



Step 12. It shows "user_group3" just created in the container "User".

Step 13. Now let's make this user "user_group3" a member of "group03". Right click "user_group3" and scroll down to Properties.

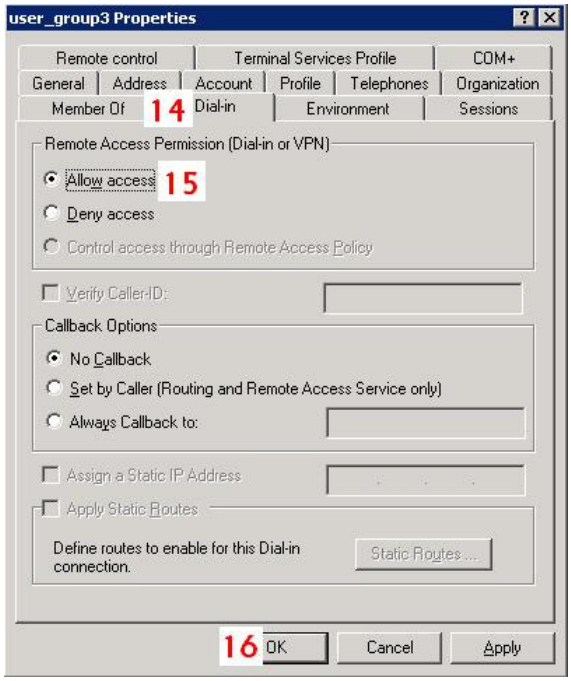


Step 14. Select Dial-in

Step 15. Select "Allow access"

Step 16. Click OK

© 2008 4IPNET, INC.



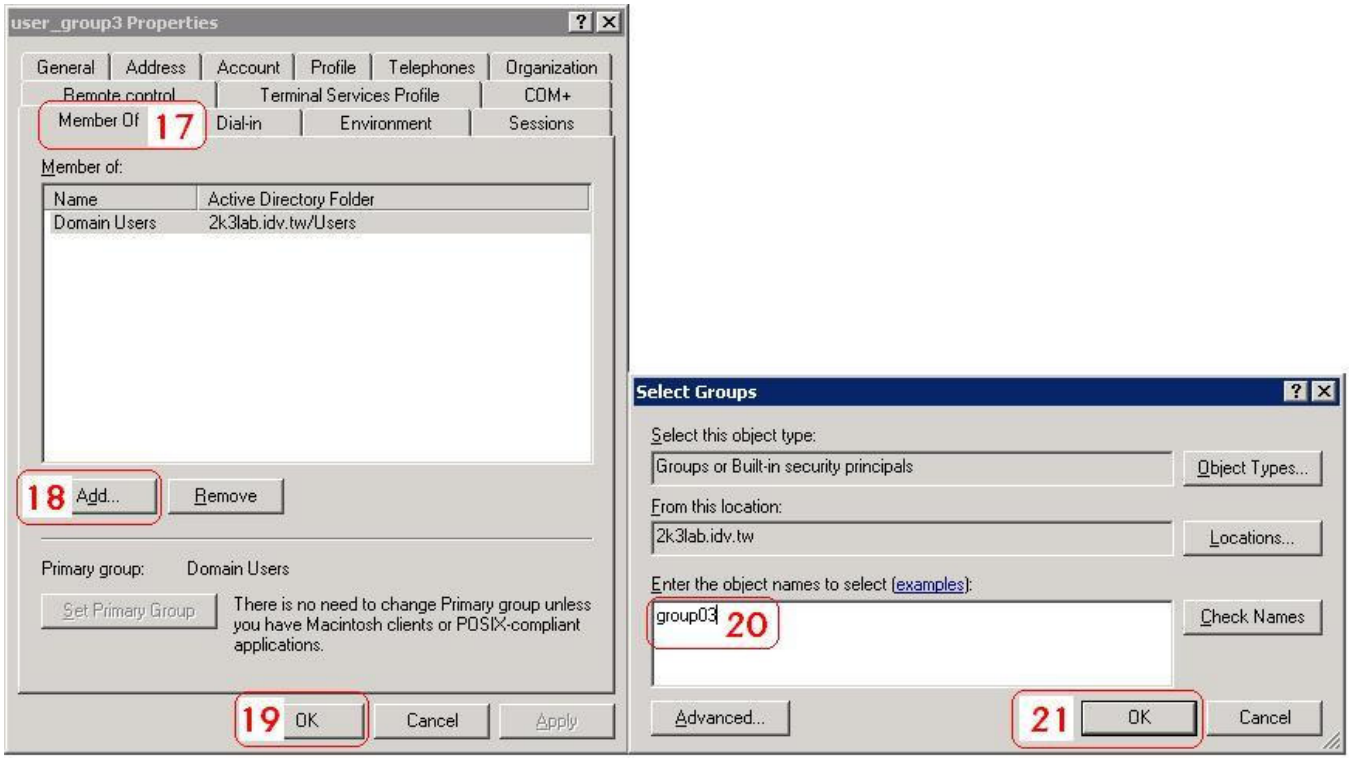
Step 17. Select "Member Of"

Step 18. Click "Add"

Step 19. Click "OK" to select Groups.

Step 20. Enter the object names "group03"

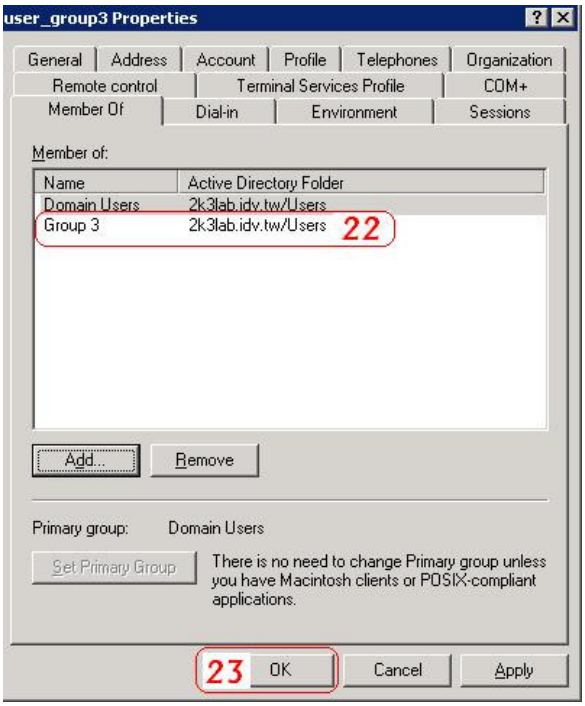
Step 21. Click "OK"



Step 22. Now this user is in "group3" under folder "2k3lab.idv.tw/Users".

© 2008 4IPNET, INC.

Step 23. Click "OK"



P/N: 10020090221

© 2008 4IPNET, INC.